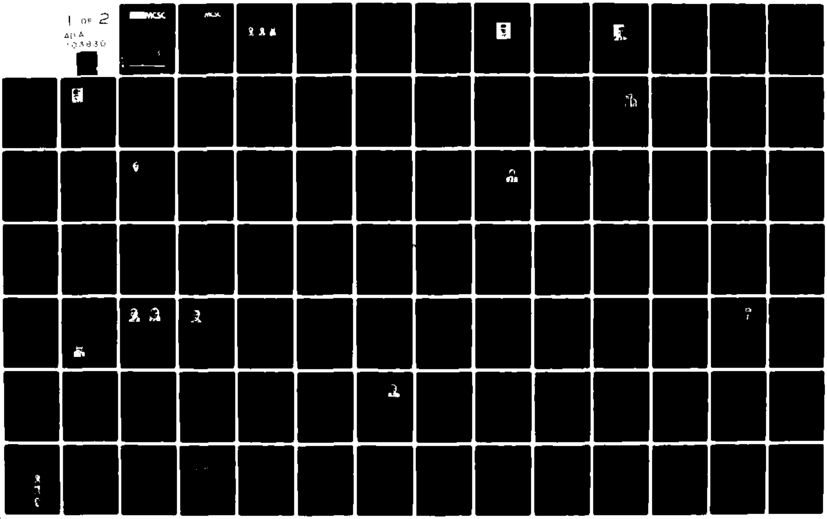
AD-A103 830 MITRE CORP BEDFORD MA F/G 17/2

PROCEEDINGS OF THE MILITARY COMMUNICATIONS SYSTEM CONTROL SYMPO--ETC(U)

NOV 80 S HARRIS, J HELLER

UNCLASSIFIED M80-30 NL



LEVEL II

AD A103830

MCSC

Proceedings of the

MILITARY COMMUNICATIONS SYSTEM CONTROL SYMPOSIUM

November, 1980

Stephen Harris & James Heller,
Editors

Proceedings of the
MILITARY COMMUNICATIONS SYSTEM CONTROL SYMPOSIUM

Sponsored by
The MITRE Corporation
Bedford, MA

Sponsored by The MITRE Corporation, Bedford, Massachusetts

MCSC

(6) Proceedings of the

MILITARY COMMUNICATIONS SYSTEM CONTROL SYMPOSIUM

November, 198Ø

(10) Stephen Harris & James Heller
Editors

(11) Nov 8Ø

(12) 14Ø

(14)

MITRE Document M8Ø-3Ø
Approved for public release; distribution unlimited

Sponsored by The **MITRE** Corporation, Bedford, Massachusetts

235050

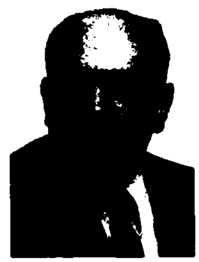
ACKNOWLEDGMENTS

The editors thank all those
who contributed to the symposium and
to the production of these proceedings.

Program Committee

Stephen Harris
The MITRE Corporation

James Heller
The MITRE Corporation



Donald Spector
Rome Air Development Center

Local Arrangements Committee

Audio	Mike Paicopolos
Budget	Melvina Johnson
Graphic Arts	Caron Shing
Plant & Facilities	Herman Schomaker
Protocol	Doris Oldfield Sue Millican
Publications	Drexel Ace
Publicity	Al Erskine
Purchasing	Dorothy Lindstrom
Publication Releases	Jim Eggers
Security	Carl Jay
Symposium Secretary	Elaine Normoyle
Registration	Susan Callahan Jean Grifoni Denise Henry
Visual	John D'Orsi

TABLE OF CONTENTS

Keynote Speaker — Maj. Gen. John H. Jacobsmeyer, Jr., USAF . . . 1

Banquet Speaker — Lt. Gen. Lee M. Paschall, USAF (Ret.) . . . 3

"Perspective on Communications System Control," Lewis S. Billig . . . 5

"Navy Force Coordination and the Requirements for Communications Network Management," Daniel M. Schutzer . . . 11

"On the Functions of a Network Management Agency," Kenneth L. Hagstrom . . . 21

"Improved Control and Technical Management of DCS Theater Assets Under Crisis and Wartime Conditions," Philip W. Fox . . . 27

"Survivability Performance of MX Communication System," N. Subramanian and I.T. Frisch . . . 33

"System Control for the Tactical/Strategic Interface," D. Spector, S.J. Iuorno, R.L. Tufaner, and W.C. Kran . . . 41

"Tactical Circuit-Switched Network Control," Yau-Wu Tang . . . 57

"Systems Control in Tactical Digital Communications Systems — A Study in Distributed Control," Lt Col James MacStravic, USA . . . 67

"The NATO III Satellite Communications Control System," M. Celebiler, N. Sanli, and E. Hirshfield . . . 75

"Network Control in NATO Integrated Communications System — Stage I," Paul A. Baiter, D.M.A., Wing Commander Keith McPhee, RAF, and David Toy . . . 83

"Evolution of Control in the Defense Satellite Communication System," P. Jeffrey Bogert . . . 97

"System Control Considerations for Next Generation DCS Switches," John W. Guppy . . . 103

"Evolving Approaches to System Control in the Defense Communications System (DCS)," L. Jankauskas and G. Wilson . . . 109

"Network Control and the CRM Make Possible Automated Digital Patching," A. Argenzia, R. Crowe, R. Krzyzanowski, and B. Simmons . . . 117

Table of Contents

"Test Systems for Base/Access Area Critical User Operational Readiness," John F. Sawyer . . . **125**

"Management of Data for Control of a Military Communication System," B.J. Leon, J.R. Monastra, and D. Spector . . . **131**

Panels . . . **137**

Demonstrations . . . **139**

INTRODUCTORY REMARKS

The papers presented at the Military Communications System Control Symposium and included in these proceedings were solicited to ensure a balanced coverage of the technical, operational, and management concepts for the control of communications systems. The papers discuss past experiences and also describe methods for meeting current and future needs.

The context for discussion of the many topics included herein may best be seen in relation to the military communications systems, existing and planned, in the European theater.

The greater sophistication of switched communications systems currently in use has increased the options available to planners regarding routing, network configuration, and traffic control. These systems are particularly valuable in contending with such possibilities as extensive battle damage, or sudden changes in traffic demands and locations due to wartime conditions. A more recent concern is the increased emphasis on interconnecting the various commercial and military systems now in use, especially in crisis situations. What are the optimal methods of controlling such complex, richly connected, and -- in some cases -- automated systems?

Some basic theoretical, simulation, and development work has been done by the R&D community. This Symposium was designed to contribute to the further development of control techniques for military communications systems.

Stephen Harris
Symposium Chairperson

Keynote Address

Major General John H. Jacobsmeyer, Jr., USAF

Major General John H. Jacobsmeyer, Jr. is the Vice Director of the Defense Communications Agency (DCA) with headquarters in Arlington, Va.

His assignments have included: Director of test and deployment for the Airborne Warning and Control System program, Electronic Systems Division, Air Force Systems Command; Chief of Research and Development Division and then Commander of the System Engineering Facility, Defense Communications Agency, Arlington, Va.; and Associate Director of the Defense Communications Engineering Center.

General Jacobsmeyer became Deputy Director, Plans and Programs, Defense Communications Agency, Arlington, Va., in June 1974. He next served as Deputy Chief of Communications, Electronics and Computer Resources, for the North American Air Defense Command and the U.S. Air Force Aerospace Defense Command at Peterson Air Force Base, Colorado, from August 1976 to September 1978. He assumed his present duties in October 1978.

General Jacobsmeyer graduated from the University of New Hampshire in June 1952 with a Bachelor of Science degree in Electrical Engineering. He earned Master of Science degrees in Electrical Engineering and Aeronautical Engineering from the University of Michigan in 1954 and 1955, respectively, and graduated from the Air War College at Maxwell Air Force Base, Alabama, in 1971.

BIANK

Banquet Address

Lieutenant General Lee M. Paschall, USAF (Ret.)

General Paschall rose through the ranks from Private to Lieutenant General. His assignments included Commander, United Kingdom Communications Region (AFCS), Deputy Director then Director of Command, Control and Communications, Headquarters United States Air Force, and for four years he was Director, Defense Communications Agency. The General retired on 1 August 1978, and presently operates his own business as a Telecommunications Consultant.

General Paschall attended the University of Colorado, graduated from the University of Alabama with a Bachelor of Arts degree in History (Phi Alpha Theta, Phi Beta Kappa) and graduated from George Washington University with a Master of Arts degree in International Affairs. He is a graduate of Air Command and Staff College, Communications-Electronics Staff Officer School and a distinguished graduate of the Air War College, Maxwell Air Force Base, Alabama.

PERSPECTIVE ON COMMUNICATIONS SYSTEM CONTROL*

Lewis S. Billig
The MITRE Corporation
Bedford, Massachusetts

We all have a vision of what system control is. The nature of that vision depends to some degree on the nature of our background in the communications field. For the purposes of this conference and this paper, I will define system control in the broadest terms possible. Basically it involves the planning, management, analysis, decisions, and technical and operational actions necessary to control a communications system so that the system is optimally responsive to the traffic and configuration requirements placed on it at any given moment.

Most military control systems are organized hierarchically. Data regarding network technical configuration, status, and traffic flows up; decisions as to actions to control and alter the network configuration flow down for implementation. To a great degree such systems currently are slow and manpower intensive. To an equally great degree, the control systems are also inhibited by lack of current information about the communications system they serve, and about the traffic on that system.

In recent years a number of studies, experiments, and acquisition programs have been initiated which have the potential to improve the response times of control systems and to reduce manpower requirements. These initiatives may also provide for better control decisions by giving the controller more complete and more timely information, and by improving his capability to analyze that information. This effort has been fragmented to a considerable degree, however. It has also been carried on without any overall understanding of the control factors operative in this closed-loop type of system.

Military communications systems must cope with a number of factors due to crisis or wartime conditions which do not affect

---

* Review of this material does not imply Department of Defense endorsement of factual accuracy or opinion.

the typical peacetime system. Such factors necessarily override the routine, and even the emergency controls and reconfigurations typical of peacetime and civilian systems. In particular, communications can be expected to be a prime target in wartime -- yet at the same time they will have to accommodate considerable increases in traffic. Moreover, the directionality of traffic will change as a wartime or crisis situation develops. Communications typically will have to depart from preplanned modes, and will be required to provide coverage in different areas and subregions. This will put heavy constraints on the communications system's capacity, coverage and survivability, and will require the system control elements to "see", analyze, and then control and reconfigure the surviving network on a near-real-time basis.

Both the physical and electronic vulnerability of U.S. (DCS) and NATO (NICS) systems have been analyzed in depth. The results dispel any myths as to their survivability. Until recently there was a reluctance to recognize, accept, and act on the fact of this vulnerability. However, the message is now getting through. Actions are being taken to reduce vulnerability by some degree of hardening, and reconstitution assets have been and are being procured and deployed. Traditional methods of alternate path selection via switch control and tech control action for priority restoral have long been planned; now the plans are being acted on. New switches, routing and signaling schemes and multiplex control systems are being acquired; once in place, these can be expected to provide a more responsive -- and in some cases even automated -- response to changing situations. The control system will be responsible for decisions as to where (based on priority), when, and how to utilize the existing and planned control capabilities, and how to optimally deploy the reconstitution assets; and, as stated, new sensing and control systems are being studied or acquired.

Given the best use of existing military communications assets, it is still recognized that an important way to achieve improved survivability, capacity, flexibility and coverage is interconnection with the national military systems such as NICS (NATO), BOXER (U.K.), GRUNDESNETZ (Germany) and ASCON (Holland). These military systems, however, have limited capacity and, of course, are designed to provide the minimum essential military capability to their own nations. Negotiations on the potential of interconnection have been carried on for many years with very limited success. The negotiations themselves are narrow in scope, with little attention given to dynamic control; most discussion has been confined to circuit swaps. Considerably more effort is required to define, in more detail, control systems for such configurations, because regardless of the success of peacetime interconnect negotiations, wartime activity will force interconnection.

Use of the switched PT&T networks as high-capacity, highly survivable systems for interconnection and/or stand-alone service for voice, data and message traffic has lately been receiving much attention. The problems involved in determining status and providing control of multiply interconnected military-civilian networks in time of war must be identified in peacetime if the composite systems are to succeed in playing their significant role -- as they have done in almost all wars.

The problems of controlling interconnected systems -- given that the systems are technically compatible -- are first political and then technical. Political decisions are liable to be driven by operational, technical, survivability and cost factors. Therefore, I believe that the communications control community must address the various options of multiple systems which are multiply connected, to provide a basis for political and technical discussions. The first priority, however, is the need to ensure "human intercommunication" among the senior military and civilian communicators of the various interested nations, to provide the confidence and understanding necessary before any nation, service or communication commander will agree to give up part of the control (and capability) of his configuration to the "greater good."

Near-real-time system control can be considered as being composed of technical, traffic, and network control. These will be discussed in more detail below; however, it is important to state here the need to develop overall basic control concepts and architecture to avoid piecemeal noncompatible implementations. The technical control function includes the functions of patching, testing, coordinating, restoring, monitoring, measuring, and reporting the status of the communication circuits traversing a station or combination of facilities. The DCS/ATEC

and the TRI-TAC/CNCE/CSCE are major sophisticated automated acquisition programs in process in this area. These programs are complex and have difficult software problems; incremental implementation is planned. Further sophisticated systems for satellite traffic control are deployed and in acquisition.

These programs are based on extensive experimentation on a low-level basis. The value of the systems, like that of most C^3 systems, and the utility of all their functions will only be truly demonstrated when they are deployed in significant quantities. In any event, these technical control systems should provide the system controller a relatively current status of the health of the network. They should also inform the local tech controller of technical faults requiring repair, alerting him to the need to patch alternate equipments or circuits to provide early restoration. These are important and expensive activities, and should be pursued and implemented in an orderly and methodical way, allowing for changes as experience is gained. It should be pointed out that integrated communications/control system survivability is essential. In particular, the practice of monitoring and controlling the network over the same communication lines used for traffic must be carefully examined to ensure independence or redundancy.

Network control, a higher level of control, involves changing the configuration of the network, in terms of both transmission and switching. Thus, if for some reason a switch or transmission path is out of order, or even nonexistent, the network controller should be able to optimize his remaining assets to provide optimum performance. This may include changes in the multiplex plan or in switching algorithms, deployment of restoral assets or even choice among interconnection options. These controls can be implemented, based on preplanned options, by means of either a patching capability or switch alternate routing. The Automatic Central Alarm System (ACAS) provides DCA Control Center at Stuttgart information on the status of various critical elements of the European AUTOVON switches. The controller could use this ACAS information if it had a better man-machine interface.

Control decisions are usually made based on preplans, or the "seat of the pants" if a direct preplan does not apply. Automated equipment for analysis and assistance in decision making should be further investigated and implemented.

Traffic control is a subset of network control and provides controls such as precedence, lineload, network in and out dialing et al. Reconfigurations of mux plans and switch routings are more drastic forms of responding to major traffic changes in quantity and directionality. Again, to a large degree these implementations are the result of preplans. However, the use and development of newer algorithms and gridded configurations may well complicate the generation of optimum instructions. Control size simulations might be valuable tools to generate pre-plan options and evaluate near-real time responses.

It can be seen, then, that the various control systems, either implemented or in acquisition, address complex problems involving significant expense and risk.

There cannot be one solution to the system control problem. Fixed facilities such as the DCS and NICS, which tend to have large coverage areas, obviously have a set of requirements different from those of tactical users who have higher mobility problems, frequent reconfigurations, and different message patterns. For example, the Field Army, deployed Tactical Air Forces, Strategic Air Forces, Naval configurations, etc., and the national military systems all have fundamentally different control requirements. Thus, we see, no solution is unique to this area. For example, the detailed designs of the ATEC and Army and Air Force CNCE/CSCE elements of the TRI-TAC are similar, yet sufficiently unlike to require different, though related equipments. In fact, the TRI-TAC had a System Control Working Group defining the needs of the services for several years. Obviously the way the services "do business" is sufficiently different so that simple, common compromises are not in the cards. As a matter of fact, the various military communications organizations led by DCA have been carrying out studies of their own in multiple aspects and sub-aspects in the area.

Another aspect impacting the system control area is the technology; satellite, airborne relay (JTIDS, MIDS, et al.), and conventional terrestrial configurations; analog, digital and hybrid, secure and non-secure, are some examples. The kind of signalling and routing (saturation signalling, right-through-control) of hierarchical and gridded switched systems also imposes

differing loads on the communication control system.

To undertake control actions without knowing their impact could possibly cause more harm than good in a complex, multiply interconnected network. Basically, then, the analytic, simulation, and experimental efforts of DCA and the services must be continued so that understanding, tools, optimal control strategies, and systems can be developed to serve the specific sorts of control configuration that exist now or can be expected in the coming communications world.

A major area of additional concern is the necessity to train people to control the complex communication networks that are on the way, such as TRI-TAC, E.T.S., NICS, et al. It is a matter for serious concern that the control systems in themselves may be so complex that the type of military people available to operate them may be a significant limiting factor. Current low-level efforts to develop operator training tools must be increased if effective operator decisions are to be expected under unusual circumstances.

In summary, the following factors must be dealt with in establishing the future decision of Communications System Control:

- The development of new and sophisticated communications systems can cause equivalent increases in the complexity of control systems.
- Control theory and understanding must be developed along with the new communications concepts, especially in interconnected systems. This will involve analysis, experimentation and simulation.
- The control system must be more reliable and survivable than the controlled system, and the requirements of wartime configurations should govern the nature of its development.
- Basic control architectural concepts should be developed in an overall context to avoid piecemeal, noncompatible implementations.
- Analysis and decision aids, as well as controller training systems, should be emphasized.

BIOGRAPHY:

Lewis S. Billig is the Technical Director of Theater Operations of The MITRE Corporation, C^3 Division, in Bedford, Massachusetts. Since joining MITRE in 1963, he has led activities related to research, design, and development of military communication systems. He has been the Director of the Planning and Systems Analysis Division, Director of Special Military Programs, Director of the Brussels Office, and Director of the Communications Systems Division.

Prior to joining MITRE, Mr. Billig held the position of Vice President and General Manager of Military Electronics at The General Electronics Laboratory. He also was on the staff of The Raytheon Company and The Martin Company.

Mr. Billig has a Master of Science degree in Electrical Engineering from Northeastern University and a B.S.E.E. from City College of New York. He is a member of the I.E.E.E. and a registered professional engineer in Massachusetts.

NAVY FORCE COORDINATION AND THE REQUIREMENT FOR COMMUNICATIONS NETWORK MANAGEMENT

Dr. Daniel M. Schutzer
Naval Electronic Systems Command
Arlington, Virginia

Command and Control is the closed-loop process that deals with the exercise of military decision-making authority over combat units. (Figure 1). This process involves the commander engaging in the following activities: planning and setting of mission objectives and procedures prior to the outbreak of hostilities; operational direction of forces both during crises and actual battle; delegation of authority and resources to subordinate commands; reconstitution and rally of forces.

Command and Control is concerned with the movement and status of military assets; e.g., task forces, task groups, ships, planes, weapon systems. This concern exists at all levels of the military command eche- e.g., command of a single ship to command of a task group, task force, fleet, ocean area, the entire Navy, on up to the Joint Chiefs of Staff. The major difference amongst command

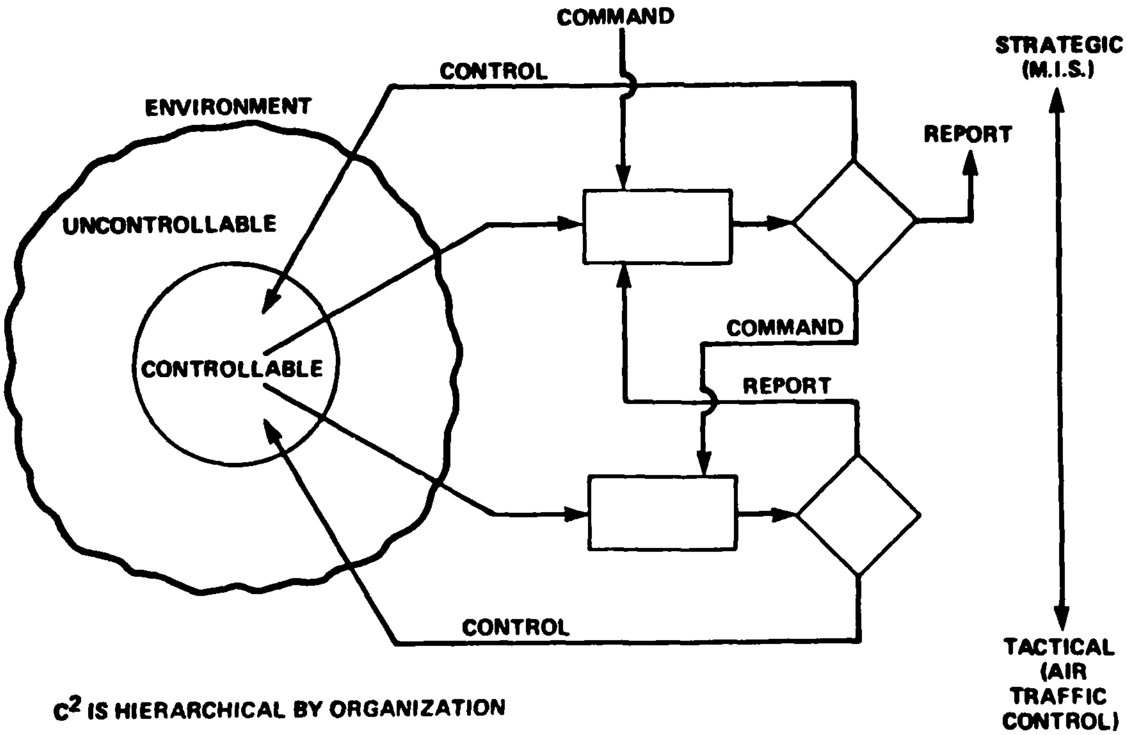


Figure 1 COMMAND AND CONTROL (C^2) IS A PROCESS

levels lies in the amount of detail and the timeliness required and the number of assets of concern. Generally, the lower the level of Command, the smaller is the region and the number of assets that are of concern, but the greater is the detail and timeliness required. Higher levels of command and control tend to be more global, strategic and planning oriented whereas lower levels of command and control tend to be more local and real-time reactive or oriented.

Each higher level of command and control must have the ability to sense, monitor and gain feedback on the state of the environment including the lower levels. This is accomplished both through direct sensing of the environment and through lower level reporting. Each level of command also must have the capability to provide direction, set objectives, and to exercise override controls on the lower levels as the situation dictates. These include controls over the coordination of warfare area activities, the allocation of platforms and weapons assets, the management and tasking of sensor and communications assets, and the state of the command and control system itself (organization structure, mission assignments, lines of command actions and information flow).

The command and control can be seen to be comprised of the four functions of:

Information Collection
Information Management
Communications
Force Management Coordination

The first three functions are performed in support of the fourth function.

Proper coordination between units can be shown to result in improved operational effectiveness (e.g., increased probabilities of detection and kill), and in minimization of unnecessary expenditure of resources (e.g., weapons, fuel). A certain level of coordination is necessary to ensure that cooperating platforms are kept informed of potential gaps and barriers in their levels of understanding and perception concerning common areas of operation and interest to a sufficient extent that these platforms can survive and operate to some minimally acceptable degree. Coordination is accomplished by monitoring, updating and controlling the various cooperating platforms actions and information products. This includes initializing a users information file when he enters new areas of operation or undertakes a new mission or application requiring greater accuracies or different/increased coverage than previously. To accomplish this level of force coordination, each platform needs an on-board Force Management and Coordination Subsystem. This Force Management and Coordination Subsystem must be capable of storing, retrieving, associating, transforming, reducing and presenting that information necessary to make effective decisions with respect to appropriate actions (e.g., controls, orders, overrides, conflict resolutions, and resource allocations). This subsystem in turn requires some kind of on-board battle area information base. This battle area information must include information on own forces, enemy and third parties.

Information on own forces is required to prevent mutual interference, fratricide, duplication of effort, fruitless expenditure of resources, and to maximize combat effectiveness.

Information on enemies is required to be able to seek out the enemy, to engage him with optimum weapons at the most advantageous time and place, and in the optimum order and to be ready to repel/defeat/attack/counter-attack.

Information on third parties is necessary to avoid wasting ordinance, to maintain a background picture, to provide protection, and to be alert to possible dangers.

These on-board data bases must be consistent throughout the entire battle force. They must draw upon all available sources to ensure the most complete and up-to-date information possible. This includes not just sources on-board and organic to the force, but also sources external to the task force.

This coordination generally requires the continuous exchange of information. Communications resources are necessary to support this information exchange.

To maintain these local information data bases requires a corresponding own ship information management system with appropriate communication linkage to other such systems both or organic and external to the task force.

Directly supporting these information management systems are the sensors. Particularly needed are sensors that can extent the combat horihorizon to the 400 nm and greater distances envisioned as required for tomorrows naval engagements. Such sensors are planned. They include a variety of upgraded and new land-based aircraft, shipboard and satellite surveillance systems. All platforms must have the communications capability to receive this sensor data both directly from the sensor systems and as processed information from correlation centers.

Communication in a military environment however is extremely fragile. It is unreliable and bandwidth limited. The challenge remains to

develop effective coordination schemes which minimize the requirement for communications resources and which can continue to function effectively over fairly long periods of unreliable communications service.

Communications can be jammed, deceived, and exploited in a hostile environment. Moreover the enemy is becoming increasingly sophisticated and proficient in these areas serving to add further emphasis and importance to this problem.

It is necessary to trade-off communications capacity for security, anti-jam protection, and/or low probability of detection and intercept. This trade-off is achieved through signal processing techniques such as spread spectrum modulation operation. Spread spectrum systems typically use an RF bandwidth which is 100 to 1000 times or more than required for the information rate.

Hostile actions can also include destruction of the available communications and command and control facilities. To overcome these sort of actions requires more autonomous local capability and less reliance on vulnerable centralized facilities. It also requires a significant investment in communications systems that can detect the onset of jamming; that can be rapidly reconstituted (quickly set-up); that can allow essential information to be dynamically rerouted along any available transmission media paths remaining (self healing) and whose available capacity can be reallocated to ensure timely satisfication in direct response to user demand on a real-time priority basis.

Demands for improved timeliness of information coupled with an increasing scarcity and cost of available skilled personnel, motivates us to build higher quality transmission/communication systems. Higher quality systems minimize the need for retransmissions and reduce the volume of messages/information received in error requiring human detection and resolution.

The above considerations result in greater costs associated with communications. This trend coupled with the increasing deployment of more sophisticated ESM/EW and sensor systems are creating a significant motivation to examine the potential for greater integration of sensor and communication systems both from a management and an interference reduction viewpoint (e.g., EMC), and from a potential cost investment and space savings viewpoint.

The Navy Telecommunications Architecture provides for three levels of communications service; namely, Minimum Essential Communications (MEC), Unimpaired Tactical Effectiveness (UTE), and Normal Sustained Operation (NSO). It is the required Minimum Essential Communication capacity that must be afforded the highest level of communications service.

Corresponding to this minimum essential communications, is a critical amount of information and command action orders exchange traffic necessary to maintain some minimum essential capability for command and control of the forces at sea. This critical amount is defined below. First, the ability to disseminate timely command actions must be assured. Second, knowledge of Location of Forces is absolutely fundamental to the command and control process. It is the common basis upon which all other information is either derived from or related to. This information is most naturally represented by a tactical situation or position plot. Knowledge of Status of Forces is the next key input to any command decision process. Simply knowing where units are is not enough. Their state of well being, and most importantly, their combat readiness is an important consideration prior to making any commitment or allocation of forces and units. Except for unusual circumstances, it is generally preferable not to commit a unit to battle that is incapable of achieving a sufficient level of combat readiness in the available time. To make an informal decision without some rudimentary knowledge of unit location is impossible. To make any allocation or

commitment of forces, or units, without some rudimentary knowledge of their respective state of combat readiness is unwise and risky. Knowledge of enemy intentions, status and capability is an equally key input to any command decision process. Finally, because of the uncertainties and unpredictability of war, some capacity must be assured for the exchange of informal fee format conversational messages, narrative record, and/or voice communications.

All command and control information and command action orders are communicated in either the form of voice, data, narrative message, or graphics. Each form offers its own particular operational advantages and disadvantages. For example, whereas voice requires greater bandwidth and exhibits less efficient information compression, it has the advantage of allowing for a rather informal, highly interactive and natural means for human communication. Data, on the other hand, is a more natural medium for computer entry, storage retrieval and manipulation. Whereas graphics represent a unique capability for presenting certain classes of information. All forms are needed, they all support command and control information exchange and manipulation.

The employment of one information form over the other is highly dependent upon the situation. Since the military situation is highly dynamic where systems fail, are jammed, and destroyed, the ability for easy and effective control and reallocation of the voice/data mix is desirable. A network over which voice and data is integrated would greatly facilitate and enhance such a capability. If voice were ultimately integrated with data in the same terminal and processors, it would represent an extremely attractive man machine interface. Imagine a system which permits side-by-side input of storage, editing and retrieval of linked verbal comments, word processing files, computer data bases and graphic presentations/ images. Economically, the revolution in digital componentry makes the consideration of a greater degree of voice/data integration over both communications networks, terminals and data processors more viable than would have been possible just a few years ago. There is also a definite advantage performance-wise in such an integration of voice and data.

Communications is the glue that ties the task force together and makes possible the effective operation of the force coordination and information management. With todays increased threat our communications links remain more vulnerable to jamming and exploitation than ever before. Compounding this problem, our communications needs are escalating rapidly. Our Navy platforms cannot afford to be outfitted with a marginal communications capability forever. Our links must be up graded in both quality (more survivable, jam resistant, more secure) and quantity (more capacity). There are programs underway to achieve these objectives (e.g., HF Improvement program, UHF AJ LOS, Joint Tactical Distribution Information System, Advanced SATCOM). Although these programs go a long way, more capable link technologies need to be developed if the future communications link quantity and quality requirements are to be met. Moreover the current communications systems must be interfaced and integrated to enable these new link upgrades to be easily introduced into Navy platforms as they are developed.

An inordinately large number of radios and antennas are necessary to satisfy todays communications needs. This is because historically, communications systems have been developed vertically in support of individual systems/users. A corresponding Electromagnetic Interference (EMI) problem exists for most ships which is barely manageable today and is likely to grow to uncontrollable proportions. Accordingly, a communications network/ link management system is needed to meet four objectives. These objectives are:

1. Allow for the evolutionary upgrade and introduction of communication links on an individual, as available basis.

2. Minimize the numbers and types of communications equipment.

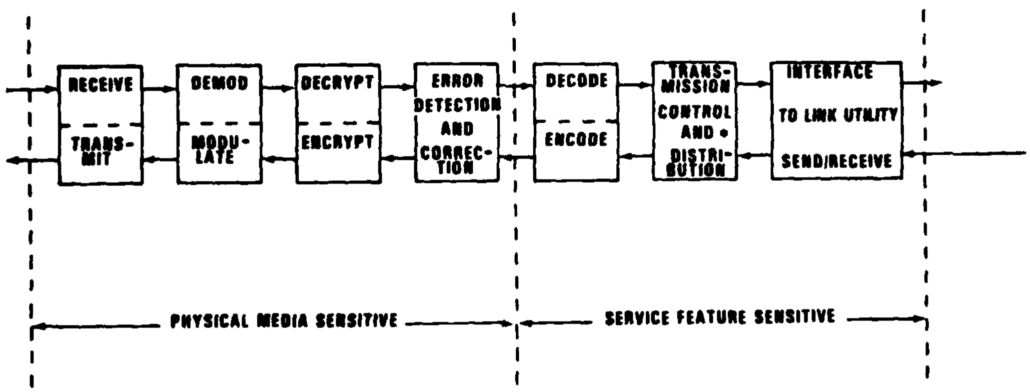
3. Reduce the potential EMI problem.

4. Improve the responsiveness, and survivability through more flexible and dynamic network and link reconfiguration, reallocation, reconstitution, and quality control.

To properly understand this network link management system, it is first necessary to study the entire end-to-end process which a data link supports. This process includes the transmission, receipt and processing of data among two or more users.

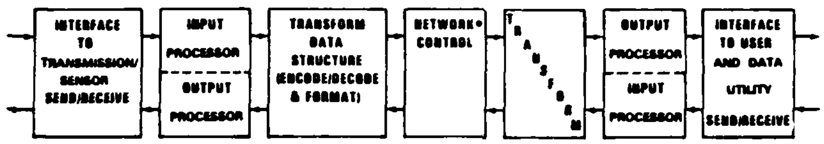
In the most general case, this process can be decomposed into three major components: a component that is sensitive to the transmission media; a component that is sensitive to the users' processes; and a generic component that is sensitive, inherently, to neither the transmission media nor the users' processes. The component sensitive to the transmission media can in turn be broken down into two major elements: an element that is sensitive to the physical transmission media characteristics and an element that is sensitive to the transmission services offered (e.g. voice, data, priority preemption, anti-jam). This is illustrated in Figure 2 including the major functions of each element. Figure 3 illustrates the generic component in terms of its major functions, and Figure 4 illustrates the user component in terms of its major functions.

It can be seen from Figures 2 through 4 that many functions get repeated over two or more of the components. These functions can be, and often are, combined to achieve hardware and processing efficiencies. These gains in efficiency are often times achieved at the expense of



* e.g., ADDRESSING, CONNECTION/DISCONNECTION, FAILURE RECOVERY, ERROR CONTROL, SEQUENCING, FLOW CONTROL

Figure 2 TRANSMISSION MEDIA SENSITIVE COMPONENT



* e.g., NETWORK ACCESS (POLLING, CONTENTION), MULTIPLEXING, SCHEDULING, PRIORITY, ROUTING, ALLOCATION, DISTRIBUTION

Figure 3 GENERIC COMPONENT

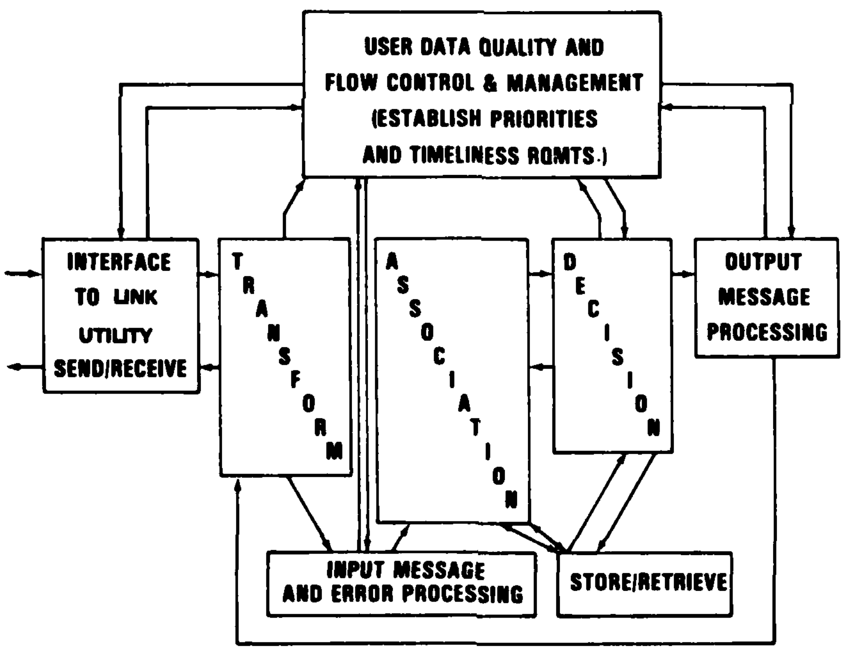


Figure 4 USER SENSITIVE COMPONENT

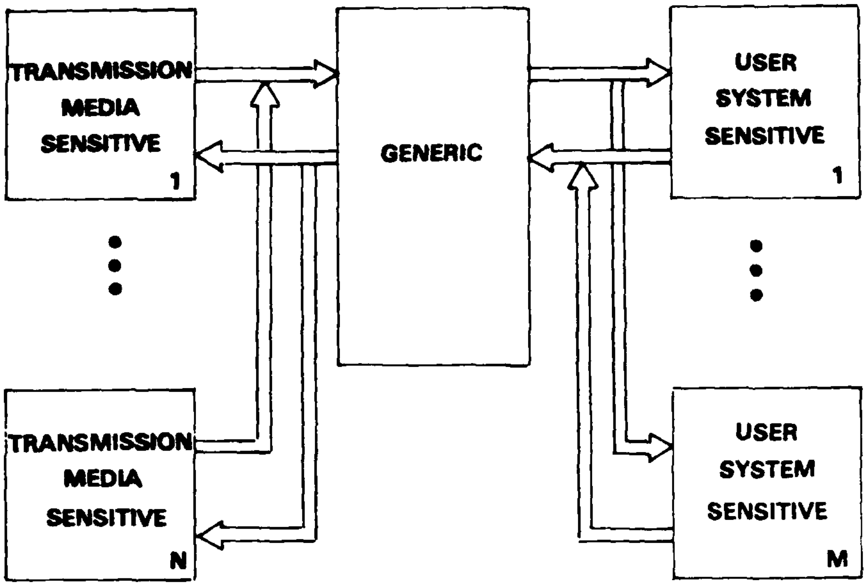


Figure 5 UNIVERSAL GENERIC COMPONENT

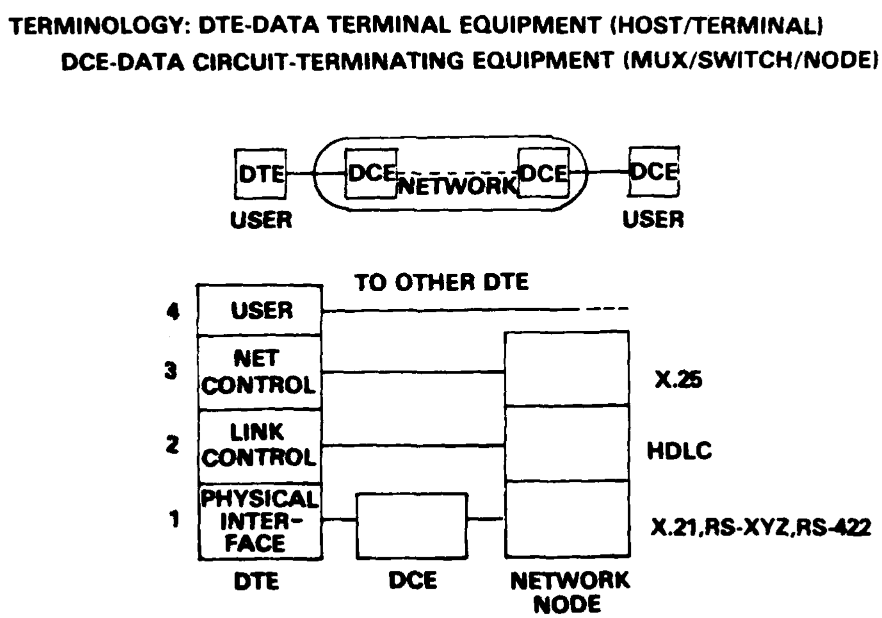


Figure 6 INTERNATIONAL STANDARDS

desired flexibilities and ease of use in system operation, and result in the potential for increased life cycle cost. For example, the adoption of a common message and header format for use by all three major components eliminates the need for as many data transformations, but must of necessity be achieved through a compromise of the optimum user-oriented message features and of the transmission-oriented message features. In many instances these compromises result in unforeseen and unanticipated hardware and processing complications that render the anticipated efficiencies in hardware cost and processing throughput at best illusionary. Furthermore, complete combination of all redundant functions/subfunctions results in the elimination of the generic component. This generic component if made sufficiently universal, as illustrated in Figure 5, affords the user the potential for greater flexibility and for interoperability with other users and with all available transmission systems. It would afford the user the opportunity to dynamically change and to introduce new force coordination communication options. Examples of such options are to vary and extend the information update periods; to tighten, loosen or otherwise modify the thresholds and criteria upon which event-by-event reporting is based; to decrease and aggregate or to increase the detail to which an event is reported. Furthermore, the suggested breakdown of functions within components, closely parallels the approach (concept of a hierarchy of protocol modules) taken in the international and national standards arena. Figure 6 illustrates the four basic protocol modules of the hierarchy; where modules 1 and 2 are seen to correspond to the two major elements of the transmission - sensitive component; Module 3 corresponds to the generic component; and module 4 corresponds to the user-sensitive component. The appropriate corresponding standards are shown alongside their respective protocol module levels. It supports the concept illustrated earlier by Figure 5; the concept that subsystems may interface at all the various protocol levels: transmission - oriented; user - oriented; and generic network oriented.

BIOGRAPHY: Dr. Schutzer joined the Naval Electronic Systems Command in the summer of 1976 as Technical Director of the Command, Control and Communications Systems Project Office. He has over nineteen years of diversified experience in government, industry and university. His areas of emphasis have been in the fields of operational research, radar, sonar, communications and computer science. Dr. Schutzer has written over forty-five publications. He has previously worked for IBM, Bell Telephone Laboratories, Sperry Rand, and the Defense Communications Agency. He has taught and lectured at both the graduate and undergraduate level at several universities including Syracuse University, Cooper Union, Fairleigh Dickenson, and Newark College of Engineering.

ON THE FUNCTIONS OF A NETWORK MANAGEMENT AGENCY

Kenneth L. Hagstrom
ITT North Telecommunications Switching Division
Cape Canaveral, Florida

ABSTRACT: This paper presents some ideas concerning the functions that must be performed by a Network Management Agency in order for it to exercise control over a communications network. The functions are described in general generic terms that apply to any network control system. It is suggested that successful network management requires all of these functions to be performed to some degree. Differences in specific control applications may result in differences in emphasis placed on the functions but all functions must be performed.

Introduction

Most of the existing literature about network or system control deals almost exclusively with either descriptions of the technical problems and requirements of system control or with suggested solutions to the control problems or possible control implementations. A review of the literature reveals:

1. there is unanimous agreement that network (or system) control is possible and necessary;
2. that there are differing views as to what is meant by the terms "network control" or "system control".
3. that there are widely differing views as to the extent to which it is possible or feasible to automate control; and
4. that there are widely differing views concerning the degree to which the control system should be distributed versus centralized.

The interchange of ideas is having the beneficial effect of leading to a better understanding of what is really a fairly large set of interrelated and complex problems called network control.

This paper does not attempt to resolve these problems but presents, for consideration, some ideas concerning the functions performed by the type of organization that must exist in order to achieve network control. For the purposes of this paper, such an organization will be referred to as a Network Management Agency (NMA) and be defined as an organization that is responsible for the planning, procurement, installation, operation, maintenance and control of a communications network. In effect, a Network Management Agency (NMA) acts as the "owner" of a communications network that provides command and control communications facilities to a community or to communities of users.

Major Functions

The tasks performed by an NMA can be grouped under six major functional headings which are:

1. Administration;
2. Training;
3. Logistics;
4. Procurement;
5. Planning; and
6. Control.

The order in which the functions are listed is not intended to imply any order of importance. The first five functions are quite often viewed as support functions for the "main" function, control of the network, but, in fact, they are equally important to the overall success of an NMA. Each function is, in its own right, a fairly complex function consisting of many sub-functions.

In the following descriptions of the functions it is important to keep in mind that what is being described are general generic functions performed by an NMA not the organizational structure required to implement them. The organizational structure of an NMA is to a large degree application dependent and will vary significantly from network to network due to differences in sizes, missions and complexities.

The Administrative Function

The administrative function provides the overall directorship and continuity of purpose of the NMA. It consists of the following sub-functions:

1. personnel administration;
2. financial control and administration;
3. security administration;
4. policy and procedure formulation;
5. handling of legal matters;
6. public relations;
7. labor relations; and
8. intersystem liaison and negotiations at the administrative level

The personnel administration functions provides for the hiring and firing of personnel, promotions and merit increases, personnel practices and employee benefits programs. It is the task of this function to see to it that an adequate and properly skilled work force is available.

The financial control and administration function provides for budget allocation and monitoring, accounting activities, cash flow control, long term budget preparation and overall fiscal control of the NMA.

The security administration function includes the formulation and enforcement of security policies, security checks and monitoring, classified material inventory and control and the investigation of security violations.

The policy and procedure formulation function sets the standards, procedures and protocols that govern the performance of all activities of the NMA. Its output is a set of standard practices documents that regulate the NMA. In most cases, many of the standard practices will be dictated by government regulations or national law. However, internal standard practices must be developed to define lines of authority and responsibility and to define how the other functions of the NMA will interact with each other.

The legal functions include negotiating contracts, terms and conditions, providing legal expertise in settling claims and disputes and representing the NMA in courts of law (if necessary).

Intersystem liaison is necessary to achieve interoperability with other systems. At the administrative level, this means setting down the guidelines to be followed during the planning and control functions.

The Training Function

The training functions provides the skilled personnel who make up the major part of the NMA work force. Regardless of the level of formal education of the people hired by the personnel administration, additional specialized training is almost always required.

This function can be divided into three major sub-functions:

1. administrative activities;
2. operations training; and
3. specialist training.

The administrative activities include the administration of the schools, class assignments and progress reports. In addition, the selection and updating of each course syllabus to reflect the current requirements of skill level is the responsibility of the training administration function.

The operations training function includes a variety of training schools and activities. These are:

1. instructor training;
2. on-the-job training supervision;
3. switch operator/attendent training;
4. field operations and maintenance training;
5. depot repair and maintenance training; and
6. installations training.

The product of the operations training function is the skilled work force that will operate and maintain the network. They represent the large majority of the work force of the NMA and perform most of the tasks of operating and maintaining the network.

The specialist training function is a difficult one to achieve because of the complexity of the specialities involved. However, the success of the NMA in performing its mission depends on having available people who understand and know a great deal about communications networks, traffic analysis, transmission systems, software maintenance and development, and complex systems operation. Because of the many years of study and training required to become proficient in these specialities, people with these skills are difficult to find. Many of the training courses necessary to produce these skills may be provided by universities under the sponsorship of the NMA. However, a comprehensive on-the-job training program will, in all probability, still be required.

The Procurement Function

The procurement function is responsible for two major buying functions:

1. replenishing supplies of spare parts; and
2. buying new equipment or subsystems.

The first function is an on-going activity required to maintain the existing network equipment. It depends on information received from the logistics function (specifically the inventory control functions) and the failure analysis and predictions of the planning function. The information supplied by these two functions makes it possible to purchase spare parts before they are needed and become critical. This is especially true for long-lead items.

The second sub-function of the procurement function is required to allow the network to grow and evolve. It is the means by which new systems and technologies are introduced into the network.

The procurement function can be divided into the following sets of activities:

Pre-contract activities:

1. technical specification preparation;
2. request-for-quote preparation;
3. proposal evaluation;
4. vendor selection; and
5. contracts negotiations.

On-going program activities:

1. contracts administration;
2. design reviews and evaluation;
3. quality assurance and inspections; and
4. vendor liaison.

Acceptance activities:

1. test and specification compliance and validation;
2. equipment acceptance;
3. facilities acceptance; and
4. licensing and certification activities.

The Logistics Function

In general, the logistics function is responsible for providing the properly skilled people with the required equipment at the right place at the right time. The activities of the logistics function are divided into two areas:

1. depot activities; and
2. field activities.

Depot activities include depot administration, depot repair and maintenance functions, equipment and parts inventory control (material control), shipping and receiving, incoming inspection and equipment and personnel deployment to support the maintenance and installation requirements of the control function.

Field activities include field maintenance and repair, equipment installation and check-out, and site spares control. The

field maintenance and repair activities are generally limited to normally unattended facilities.

The repair and maintenance activities of manned sites is performed under the direction of the control function.

The Planning Function

The planning function is one of the major sources of information for the other functions. Most of the decisions made in performing the other functions will be based on information provided by this function.

The planning function is divided into four major sub-functions as follows:

1. performance analysis;
2. resource management;
3. system development; and
4. operations control.

Performance analysis uses the statistics collected by the control function to assess overall performance. It includes the following major tasks:

1. current network performance analysis, i.e., how well does the existing system perform and does it meet requirements;
2. current user requirements and network utilization analysis, i.e., are the users' requirements being met and are they utilizing the capabilities of the network. Part of this analysis includes human engineering considerations such as determining whether the system design is so complex that it leads to user operational errors;
3. network traffic analysis, i.e., end-to-end grade of service, speed of service, probability of preemption, user traffic patterns, network congestion patterns, etc.;
4. equipment performance analysis, i.e., measured failure rates, actual availability calculations, failure analysis, actual mean time to repair, etc.;
5. network simulation and analysis for long term performance assessment and damage scenario planning; and
6. fault simulation and analysis to determine the actual cause of major faults, i.e., whether hardware or software bugs or a combination of the two.

Resource management uses the results of the performance analysis to perform the following tasks:

1. contingency planning, i.e., formulating plans to counter the effects of equipment outage or network damage;
2. maintenance philosophy and procedures formulation;
3. network topology planning, i.e., planning changes to the networks' topology to increase survivibility, reduce traffic congestion and accommodate new requirements; and
4. node configuration planning, i.e., the addition of new users to nodes, the adjustment of common equipment pools to meet actual traffic demands, etc..

System development planning is based on information obtained from the performance analysis and resource management functions and includes the following tasks:

1. future network requirements analysis, e.g., the addition of new nodes or transmission links to the network;
2. future user requirements analysis, e.g., the addition of new call features;
3. technology surveys to keep abreast of the current technological developments and how they may apply to meet future requirements;
4. new equipment specification definition, i.e., defining the specific technical and performance characteristics of the required new equipment;
5. new facilities specification definition.

Operations control provides the planning necessary to control the following:

1. data base assembly and validation which includes allocating system features to users such as precedence or conference privileges;
2. radio frequency allocation to avoid unwanted overlapping or inadvertent radio interference;
3. intersystem interface requirements definition to ensure interoperability;
4. intersystem liaison at the planning level to work out the details of interoperability;
5. communications security (COMSEC) planning to determine the correct placement of the equipment, key change procedures, etc..

The Control Function

The control function provides the dynamic near real-time control of the network. It operates on information collected from the network in accordance with the procedures and plans of the planning function. It consists of five major subfunctions as follows:

1. data collection;
2. performance assessment (near real-time);
3. performance adjustment (dynamic control);
4. maintenance direction and control; and
5. operations control.

The data collection functions are of major importance since these statistics are the basis for most of the decisions made by both the planning function and the control function. These activities include:

1. traffic statistics collection and storage;
2. equipment status statistics collection and storage;
3. failure report collection and storage; and
4. performance monitor/test report collection and storage.

The performance assessment function uses the statistics gathered by the data collection function to determine the real-time or near real-time performance of the network. These activities include:

1. first order traffic analysis, i.e., an analysis sufficient to identify traffic congestion areas;
2. first order equipment status analysis, i.e., an analysis sufficient to determine whether or not rerouting around failed equipment is necessary;
3. network simulation, i.e., simulation based on current traffic and equipment status statistics to determine the best course of action to alleviate the problem(s).

The performance adjustment function consists of the control actions taken in response to the performance assessment output to improve network performance. These activities include:

1. control commands dissimination;
2. command response analysis;
3. traffic routing management;
4. traffic load control implementation; and
5. contingency plans implementation.

The maintenance direction and control functions are those maintenance activities performed by the on-site personnel in response to published policies, local alarm indications or commands from control centers. These activities include:

1. preventive maintenance;
2. remote maintenance and diagnosis; and
3. local site maintenance and repair.

The operations control function implements the operations control plans of the planning function. These activities include:

1. data base management and dissimination;
2. radio frequency allocation control;
3. COMSEC control and management; and
4. intersystem liaison at the control level.

Concluding Comments

The set of functions described above include all functions required to operate, maintain and control a command and control communications network. These functions do not reside in a single location but permeate the entire network, i.e., they are dispersed throughout the entire system. This is particularly true of the control and logistics functions.

Implicit in the descriptions of the NMA functions is the fact that the network control system, the SYSCON system, is completely integrated into the overall system. When viewed separately, the network control system appears as a hierarchial structure superimposed on the grid (or mesh) structure of the communications network.

The six generic functions of an NMA are each quite complex. Fortunately, many of them can be and probably should be automated or semi-automated. The problem lies in determining what should be automated to some degree. It appears that both too little and too much automation lead to unmanageable networks. Too little automation is unmanageable because too many people must make too many decisions too quickly. Too much automation is unmanageable because additional systems must be incorporated to manage the automated managers.

BIOGRAPHY. Kenneth L. Hagstrom is the Director of Military Systems Design for ITT/North Telecommunications Switching Division. Since joining ITT/North in 1970, Mr. Hagstrom has been involved in designing military telecommunications equipment. He is the chief architect of the NTX-2000 switching system currently being installed in NATO nations. The NTX-2000 switches will be the switching systems used in the NICS IVSN.

Mr. Hagstrom was previously with Texas Instruments where he was involved in the design of VOCODERS, PCM and PDM multiplexing equipment.

Mr. Hagstrom holds a Bachelor's degree in Physics from the University of Texas at Arlington. He is a continuing member of Sigma Pi Sigma.

IMPROVED CONTROL AND TECHNICAL MANAGEMENT OF DCS THEATER ASSETS UNDER CRISIS AND WARTIME CONDITIONS

Philip W. Fox
Computer Sciences Corporation
Falls Church, Virginia

ABSTRACT: This paper discusses improvements to the DCS System Control (SYSCON) Subsystem that can enhance the performance of the Defense Communications System (DCS) under crisis and wartime conditions.

The paper identifies a 1985 baseline SYSCON subsystem with its elements, operational constraints, and basic control concepts; summarizes an analysis that identifies SYSCON improvements for operation under stress conditions; and presents a suggested DCS SYSCON architecture.

INTRODUCTION

Within the DCS, SYSCON functions manage network assets and provide a critical service that permits the networks to respond to user demands for service under all conditions and levels of stress. It is therefore essential to the survivability of the DCS and its services.

SYSCON manages the network assets by assuring efficient use of all capacity for the full complement of provided services. New users or on-demand users must be handled concurrently with full period users. The network manager must provide the user with service and connectivity to command and control as well as administrative users. SYSCON elements, located at various levels in the network structure must be responsive to the user demands.

To be considered survivable, network services must be available to users during the period of greatest demand: stressed conditions. Therefore, the SYSCON functions themselves must be survivable. The heart of DCS management, which provides the user the essential services for command and control is SYSCON. Although necessary for survivability, SYSCON alone is not sufficient to provide the required

level of network survivability. It, however compared to network diversity or hardening approaches, is a very cost effective approach to resolving the problem.

Planned connectivity for each of the transmission systems, and communications networks for 1985 has been identified. Emphasis must be placed on defining the assets of those communications links which will exist to support the SYSCON subsystem, i.e., Critical Control Circuits (CCCs), and Orderwires (OWs). It is these links which influences the operation of the SYSCON subsystem during a crisis, and therefore must survive any degradation in service cause by that crisis (natural or man made).

This paper addresses the problem of how to provide the necessary survivability to the DCS for the 1985 time frame by presenting suggestions for enhancing the performance and the survivability of the DCS SYSCON subsystem.

The paper is organized as follows: (1) Baseline SYSCON subsystem definition; (2) Identification of Potential Improvements; (3) Analysis of Improvements and Recommendation of an architecture for an improved DCS SYSCON subsystem.

BASELINE DESCRIPTION

The DCS SYSCON subsystem is currently organized in a hierarchical structure, known as the DCA Operations Control Complex (DOCC). There are five levels in the SYSCON hierarchy, the first two levels and part of the third, make up the DOCC: (1) Worldwide Control is performed by the DCA Operations Center (DCAOC) in Arlington, Virginia, which includes the planned DSCS Operations Control System (DOCS) Operations Control Element (OCE), the AUTODIN II Network Control Center (NCC), and utilizes the Worldwide On-Line System (WWOLS) computer network; (2) Theater Level Control is performed by Area Communications Operations Centers (ACOCs) for the Western Hemisphere, European and Pacific Theaters, which includes the planned DOCS OCEs, the experimental AUTOVON Network Control Program, and the WWOLS; (3) Regional control is performed by DCA operated Regional Communications Operations Centers (RCOCs), Facility Control Offices (FCOs), for the planned Automated Technical Control (ATEC) System the ATEC Sector Control Subsystem (SCS) and the planned DOCS DSCS Operations Centers (DCSCOCs); (4) Intermediate control is performed by Intermediate Control Offices (ICOs), the planned ATEC Nodal Control Subsystem (NCS), and major Technical Control Facilities (TCFs); and (5) Station control is performed by Circuit Control Offices (CCOs), AUTOVON switching centers, AUTODIN switching centers, the planned ATEC Monitoring and Alarm System (MAS), the planned DOCS Terminal Control Element (TCE), and TCFs.

Control Functions

The system control functions which are required for crisis management, are derived from two sources.

First, a generic model of a control system can be identified which represents the basic SYSCON functions. These generic functional elements are the following: (1) system status reporting; (2) system data reduction and analysis; (3) configuration and control decisions; (4) issuance of configuration and control directives; (5) coordination with external control elements; and (6) coordination among operational (controlled) elements. The relationships of these elements are depicted in Figure 1. Multiple circuit outages which begin to impair elements 1, 4, 5 and 6 are communications dependent. Without the ability to gather status, coordinate with other control elements, and issue control directives, the information processing functions (elements 2 and 3) become ineffective. Isolating an information processing capability from the system, results in the same disruption of control functions as loss of the information processing capability itself. In either of these cases, coordination directly among operational elements becomes the only means to provide a very limited capability to perform system control activities. To combat this possibility, the problem then becomes one of ensuring the survivability of the system control functional elements. In order to do this the physical system control structure capabilities required to supportthese functional elements must be made survivable with regard to the stresses that may be applied to the DCS. The preservation of elements 1, 4, and 5 requires a survivable critical control circuit network. Elements 2 and 3 depend upon the survivability of control facilities, especially ADP related capa-

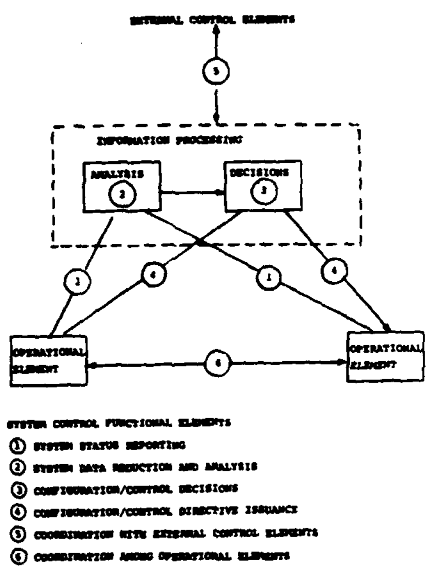


Figure 1. Generic System Control Model

bilities. Element 6 is dependent upon the DCS orderwire network and therefore depends upon the redundancy of communications connectivity between/among operational elements.

Second, through discussions with the engineering and control staff members at each of the major DOCC operations centers, the essential functions were identified. Consequently, eleven separable functions have been identified from those functions performed by DCA operations center staff as being those required to support the model functions. The eleven functions fall into three categories and are: (a) Communications Connectivity Management (1. Circuit Restoral, 2. Circuit Allocation and Engineering, 3. Reconstitution, 4. Extension/Augmentation of the DCS, 5. Reconfiguration, 6. Contingency Plan Management); (b) Status Collection and Retention (7. Data Base Management); and (c) Network Control (8) Satellite Network Control, 9. AUTOVON Traffic Control, 10. AUTODIN Traffic Control, and 11. AUTOSEVOCOM Traffic Control).

Stress Conditions

The stress conditions listed above occur during a crisis or wartime period and will require system control actions to be taken. The planned SYSCON control subsystem assets (AUTOVON Control, AUTODIN Control, WWOLS, ATEC, and DOCS) were analyzed to derive the shortfalls of these assets in support of those functions. Special operational (political, logistical, and tactical operations) considerations were identified which would be important in the production of recommended approaches to improve the survivability of the control subsystem functions. Stresses during peacetime, pre-conflict, and conventional war periods have also been considered. Further, stress and vulnerability relationships identified in a DCA vulnerability study (COMSTRESS) have been incorporated. In summary, the next step to develop approaches, discussed in the next paragraph, for improving the performance of the control system during a crisis is based upon existing system constraints, shortfalls, and typical stresses which could be applied to the DCS during crisis periods.

Centralized vs. Decentralized System

During peacetime centralized SYSCON will enhance the efficiency and operational effectiveness of the DCS. This centralized philosophy is attractive even during those circumstances associated with minor cirsis conditions, such as those causing localized network damage (i.e., natural or man made). A centrally controlled SYSCON has the distinct advantage of overseeing the larger DCS network, optimizing effective solutions to alleviate the crisis, and can take advantage of the inherent adaptability of the DCS to make the necessary adjustments. An example of this type of problem is represented by a single AUTOVON switch failure that must be resolved by alternate routing circuits around the damaged equipment. Due to the technology employed in AUTOVON controls, the logical coordinator and executor of SYSCON is the DCA Area Communications Operations Center (ACOC).

At the other extreme from peacetime, that of some general wartime condition, it is desirable to have the DCS decentrally managed. There are two important reasons for this conclusion. First, during times

of severe stress the DOCC is likely to be damaged, and therefore architecturally fragmented. Under such circumstances a decentralized SYSCON subsystem will allow many of the fragmented substructures to continue to operate in an effective manner serving a localized area. The second compelling reason for decentralization under severe crisis has to do with the fact that under wartime conditions the DCS becomes part of the theater commanders' assets. As the military threats become more severe, the operational commands themselves become less centrally controlled, fragmented and, of necessity, independent. The regional, intermediate or station level assets of the DCS servicing a particular level of command may become disconnected from the DCS. This also affects the DOCC, at large, along with the associated military subscribers' assets.

In between these two extremes, the DCS would operate in varying forms of centralized control. That is, as a given scenario transitions from peacetime to general tactical wartime conditions, the DCS will likely transition from a largely integrated and centrally managed system, to a largely fragmented and locally controlled set of subnetworks. The key SYSCON issue is how to architect such a transition smoothly

IMPROVEMENTS CONSIDERED

Several approaches can provide sufficient improvements n the SYSCON subsystem to be able to respond to a crisis, they address the specific constraints which are imposed by the nature of the DCS itself. Serious consideration is given to minimum cost to achieve the goals set forth. Each of the approaches alone does not provide sufficient improvements to the control system for survivability. Therefore, the following discussion of each approach considers the improvements to be implemented as an integrated system.

Increased Survivability of CCCs and OWs

In order to support the collection of status information and issuance of control decisions, the CCC and OW networks must be made survivable. *If status and decision* information transfers cannot be effected, then, the control system cannot be effective. Approaches to improving these networks include improving survivability of transmission elements which exist, addition of new elements, and making better use of existing elements. This can be accomplished by eliminating some of the single threadedness of the CCC and OW networks, and utility of a mix of transmission media for CCC and OW traffic.

Near Real Time ADP System Control Tools

The Analysis and Decision Making functions are not currently capable of being performed in time to be effective in crisis periods. The Communications Connectivity Management, Status Collection and Retention, and Network Control Functions are currently supported by a combination of manual procedures and inadequate computer based tools to be effective. Therefore some ADP tools will be required to improve the ability of controllers and engineers to make decisions and issue control directives to the operational elements and network switching elements. The requisite ADP tools should be capable of collecting status information, providing network controllers with information about status which affects critical users, and displaying decision options available to network controllers when losses in service occur.

Continuity of Operations Center Capabilities

Although contrary to the trend of implementing network controls in a distributed manner to manage systems which are somewhat survivable due to their inherent design and redundant capabilities, the DCS networks (AUTOVON, AUTODIN and AUTOSEVOCOM) each require a single site from which control actions are coordinated from and control decisions made. Moreover, due to the nature of the operational procedures used for technical control of these networks and their use of the transmission media (satellite, terrestrial, and submarine) integrated control of all of the networks and transmission media is the most efficient approach for crisis management of the DCS. Therefore, theater level control (ACOCs, and RCOCs) must be survivable in order to effectively manage these assets. Although control actions for these networks and media can be effected from many different sites it is significantly less effective than an integrated approach to control. Approaches to insuring that theater level control which were consider-

ed included: Redundant ACOC, DCAOC backup of ACOC, Hardened facilities, NATO Central Operating Authority (COA) Backup of ACOC, Joint (NATO COA and ACOC) Communications Operations Center (JCOC) Concept, and expansion of the number of Regional Communications Operations Centers (RCOC). Further, each DCS theater imposes a different set of constraints on a solution and must be considered independently of the others. European Theater control must be maintained within a small area when compared to the Pacific Theater. In the Pacific Theater, communications assets tend to be divisible into islands of communications assets with long distance connections. The European Theater, on the other hand, is not easily divisible, as such. It is a highly intertwined set of assets. In contrast to the European and Pacific Theaters, WESTHEM control is primarily concerned with interfaces to AT&T and Western Union control centers, since all WESTHEM assets are leased from these carriers.

Increased SYSCON Responsibility at ATEC and DOCS Elements

Although some survivability is achieved by ensuring that the centralized control centers will exist, it is not sufficient. Distribution of functions must still be made. Moreover, there are several sites, in each theater which have the potential to become sites to which control functions can be distributed. Included in these sites are ATEC Sector Control Subsystems, and DOCS DSCS Operations Centers. Each theater will have at least four SCSs and one DSCSOC. There exists the capability at each site, due to the existence of computer equipment, connectivity to a substantial portion of the DCS, and some engineering staff to support the required missions. Approaches to implement the distribution of functions to these control sites were considered, and several concepts of operation were identified.

ATEC Survivability and Crisis Mode

The programmed ATEC system can play a major role in the SYSCON subsystem due to its network of distributed computing equipment and connectivity to DCS assets. The ATEC system can be most useful in satisfying the need to collect status information and issue control directives. However, the current design of the ATEC system is not adequate to support near-real-time data collection needs of the SYSCON subsystem during a crisis. The hierarchy of control provided by the ATEC system is not survivable because it is single threaded, and only minor provision has been made to recover from station, node or sector facility outages. The provision for saving outage status at the severed node will only permit the fragmented portion of the DCS to be utilized in crisis decisionmaking. If the severed node could be reconnected, a prolonged period of utility of a larger data base for control decisionmaking will result. Other problems exist with the ATEC design, e.g., no automated reporting of theater level status information has been provided, and no automated reporting of station level status data will be made. Manual procedures will be used to perform these functions. Changes to the ATEC system can be made to make the system survivable. For example, if a Sector is inoperable, all real-time reporting from nodes and stations which are in that sector is lost. The remaining Sectors should be made capable of receiving and maintaining status information from the surviving nodes and stations. The nodes can be connected to another sector or to the ACOC via the use of AUTODIN or using acoustic couplers for transmission over AUTOVON circuits. A second major change to ATEC can improve the response time of the status collection process. This is via the concept of a crisis mode of operation. In this mode, the ATEC station level equipment would be programmed to perform full monitoring of circuit and equipment parameters on mission essential circuits. Other non-essential circuits would be monitored for major alarms only. This crisis mode can be tied to the ADP System Control tools defined above as follows. Suppose that a restoral plan is generated. The preempted non-essential circuits require full monitoring at this time. Therefore a further enhancement of the near-real-time ADP System Control tools, as part of generating a restoral plan, the ADP tools would generate the preempted circuit list and the directives to the ATEC station equipment to monitor these newly defined essential circuits, and direct the equipment to monitor with the appropriate thresholds for alarms based upon the new service being provided by the circuit.

CONCLUSIONS

A more responsive, survivable DCS SYSCON subsystem must include each of the improvements identified above.

First, ACOC Continuity of Operation and distribution of control are the most important improvements. There must be control facilities at selected location(s) which are charged with the authority to make management decisions. This enhancement recommends the requisite functional elements of both alternative ACOC's for minor crises, and distributed control for major crises. Second, CCC and OW network survivability is next in importance because the control site must be able to collect data and disseminate control decisions to stations and network switching centers. Third, near-real-time ADP tools are required to assist controllers and engineers in analyzing problems and making decisions. Timely decisions, an accurate data base and system traffic status is essential to fulfill control missions and perform the essential functions. These three improvements are closely related and each must be implemented for fully responsive control.

The remaining improvements are subsets of the above recommendations. First, increased distribution of responsibility is directed toward improving the theater level continuity of operations plan by exploiting computing hardware available at a level close to the operating elements. Both ATEC and DOCS can provide such support. Second, the ATEC survivability/crisis mode approach is supportive of both the CCC survivability and ADP tool improvements. ATEC provides status reports on the DCS assets, therefore reporting time can be reduced, and data base drift minimized. Further, the crisis mode can expedite the reporting of mission essential circuit status by reducing the measurement time by ATEC station level equipment.

Specific recommendations for each DCA theater must be implemented independently in each theater, since each has unique characteristics and shortfalls to be considered.

ACKNOWLEDGEMENT

This work has been performed for the Defense Communications Agency, Defense Communications Engineering Center (DCEC) by Computer Sciences Corporation (CSC) under Contract Number DCA100-79-C-0021.

BIOGRAPHY. Phillip W. Fox is the Manager of Computer Sciences Corporation's C^3 Crisis Management Department, based in Falls Church, Virginia. He has a broad background of experience in the DCS, WWMCCS, NMCS, MEECN, Tactical, and supporting systems. With expertise in Communication Systems Engineering, Computer Systems Engineering and Military Operations, he has been responsible for systems engineering, analysis, and investigation of complex system requirements such as vulnerability, survivability, network architecture, system control, procedures, concepts, designs, computer engineering, networks, simulation, new technological developments.

SURVIVABILITY PERFORMANCE OF MX COMMUNICATION SYSTEM

Narayan Subramanian & Ivan T. Frisch
Network Analysis Corporation
Great Neck, New York

ABSTRACT: A simulcast radio network, using priority reservation, is described for the MX command and control system. Simulation results on network survivability and reaction time are given for a typical wing deployment. The broadcast routing associated with simulcast requires no control or monitoring overhead since all nodes act as relays. However, this requires strict control of traffic entering the network. This is done by imposing a prioritized reservation channel access control protocol.

INTRODUCTION

This paper describes a communication control strategy based on the "shell-game" approach of deploying about 250 missiles randomly among 5,000 shelters. In the post-attack mode, communications is required only between occupied surviving shelters. A survivable MF radio system has been considered to meet the postattack Command, Control, and Communications (C^3) requirements. We describe a network architecture for the C^3 network that will:

- Provide a survivable, flexible, and robust routing procedure;
- Provide controlled access to the channel with no contention;
- Use broadcast transmissions to ensure "Preservation of Location Uncertainty" (PLU); that is, prevent enemy detection of live missile locations.

Simulation results are given for the survivability performance of a wing-wide C^3 network operating on the simulcast protocol.

For the present study, we assumed the 5,000 shelters, comprising the wing, are divided into five, roughly equal sized squadrons, each with an MLCC (Missile Launch Control Center), up to two ALCCs (Alternate Launch Control Centers). Gateways interface the MX system to External Higher Authority.

SIMULCAST SYSTEM

In its basic form, simulcast is a broadcast routing scheme in which a station transmits a message in a reserved time slot, and every station that receives this transmission correctly will rebroadcast the message in time synchronization during the second time slot; stations receiving the message in the second slot repeat during the third slot. The message thus propagates through the wing on a hop-by-hop basis, similar to ripples spreading across the surface of a pool. To control access to the channel, a reservation slot is provided. Each station is allotted a mini-slot within the reservation slot. If a station has a message to send, it broadcasts a short reservation message in its reservation slot and lets it propagate through the network according to the simulcast hop-by-hop repeat rule, to ensure that all stations receive the reservation request. The station gains access to the channel at the end of the reservation slot and transmits its message without contention from other stations. Figure 1 illustrates the simulcast protocol.[1]

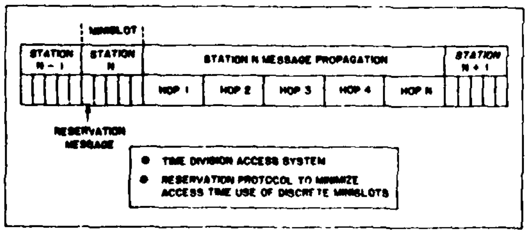


FIG. 1: SIMULCAST CHANNEL PROTOCOL

The principal advantages of the simulcast system are:

1. Broadcast routing is simple. No routing information is needed in the message or at the repeating stations since each station repeats every correct message it receives (messages are repeated only once). This also facilitates the preservation of location of uncertainty (PLU).
2. Broadcast routing is a natural scheme to meet the requirement that every C^2 message is received by every surviving missile.
3. The protocol is robust since every station acts as a relay, thus providing a very high degree of redundant paths.
4. Network management is easy since only one message is "active" at any time.
5. It provides uniform equipment and operating conditions.

In addition, the simulcast protocol can also provide significant advantages in establishing network connectivity across a "swath attack;" that is, an atack that attempts to destroy all nodes in a swath to prevent communications across the detroyed area. The multiple, simultaneous repeats of simulcast may result in either a power gain or power loss, depending on the relative phases of the arriving signals at a receiver. Since there will be a large number of receivers on either side of a swath, the probability of power gain for at least one receiver is very high. Since any receiver can act as a relay, it is possible to bridge the swath and maintain network connectivity in an adaptive manner.

SIMULATION MODEL

A comprehensive model of the simulcast concept has been developed to study the performance of the simulcast system. This model includes the following network characteristics:

a. RF propagation loss over smooth earth;
b. Signal attenuation due to mountains;
c. Combining of signals from several transmitters;
d. Antenna patterns;
e. Variation in signal phase relationships due to frequency hopping;
f. Wing geography;
g. Number and location of stations;
h. Propagation of messages through the wing on one and two channels.

The model includes a detailed topographic data base of an MX wing site in Continental United States. This data base includes wing boundaries, mountain contours, and potential missile shelters.

SURVIVABILITY PERFORMANCE EVALUATION:

The survivability criterion for the C^3 network is the percentage of stations that receive a message. If N_i stations receive a transmission by Station i, then the C^3 network survivability measure for this station is:

$$S_i = \frac{N_i}{N - 1}$$

Where N equals the total number of surviving missiles in the wing. The average network survivability is:

$$S = \frac{1}{N} \sum_{1}^{N} S_i$$

$$= \frac{1}{M} \sum_{1}^{N} \frac{N_i}{N - 1}.$$

To obtain insight into the impact of parameter variation on the system performance, the following outputs are generated:

1. The average network survivability which is a measure of the connectivity of the network and is equal to the average number of surviving missiles that receive a C^2 message.
2. The average "reachability" or message hop distribution.

The average reachability describes the simulcast hop-by-hop propagation pattern. The average reachability in hop i is defined to be equal to the average percentage of surviving missiles that receive a C^2 message in that hop.

Figure 2 is a graphical output of the program showing the hop-by-hop simulcast propagation across a rugged mountain terrain. Connectivity across obstacles such as mountains is achieved either directly due to the signal reinforcement from multiple transmissions or by using relays.

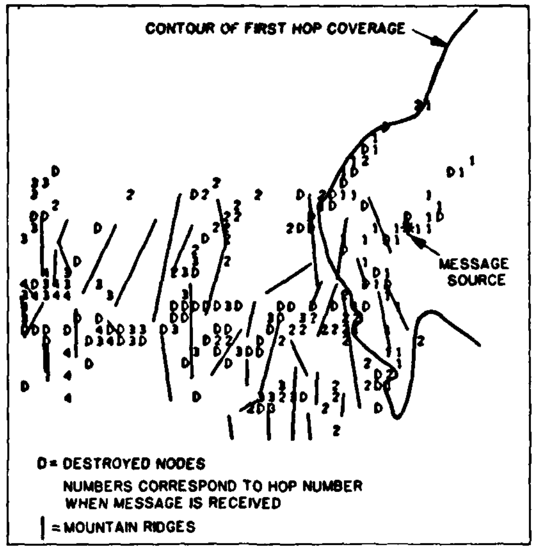


FIG. 2: SIMULCAST HOP PATTERN

Figures 3 and 4 represent typical results of the parametric studies on survivability performance. The two key parameters that were varied are radio range and attack level.

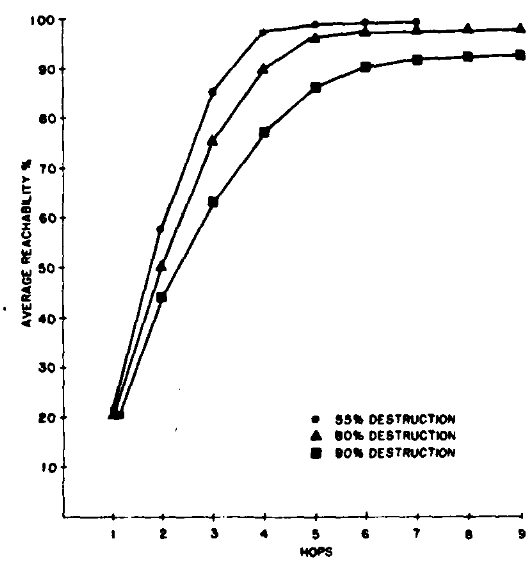


FIG. 3: SIMULCAST PERFORMANCE AT 30 KM

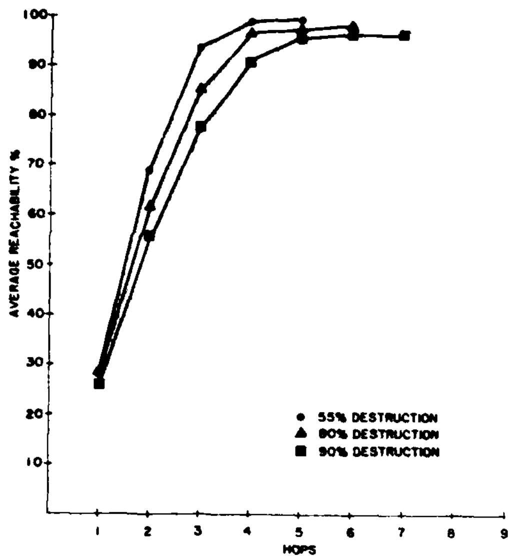


FIG. 4: SIMULCAST PERFORMANCE AT 50 KM

The results show that the network survivability is quite robust with respect to radio range and attack level. For example, with a 55 percent attack (that is, an attack that destroys 55 percent of the nodes), the number of hops required by a message to cover over 90 percent of the wing is four, with variation in the radio range between 30 kilometers and 70 kilometers. This surprising result can be explained by the fact that the range advantage provides increased coverage in the first hop, but the margin decreases in subsequent hops due to the large number of relays. Table 1 shows the number of transmitting stations in each hop for radio range of 30 km, 50 km, and 70 km. It is seen that the higher radio range provides increased coverage in the first hop, but the large number of relays compensates for this in the subsequent hops for the lower radio ranges.

TABLE 1: PERCENTAGE OF SURVIVING STATIONS RELAYING MESSAGE

	RADIO RANGE		
Hop No.	30 km	50 km	70 km
1	22	28	36
2	36	40	46
3	27	26	16
4	12	4	2
5	3	2	--

Figure 5 shows the survivability performance under a swath attack, in which the wing is partitioned as shown in Figure 6. It is seen that the simulcast protocol provides for a fully connected network by using signal reinforcements from multiple transmissions to penetrate the destroyed swath.

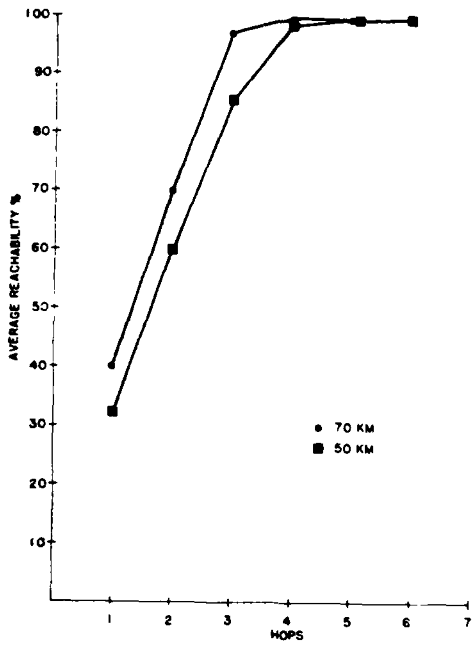


FIG. 5: SIMULCAST PERFORMANCE UNDER SWATH ATTACK

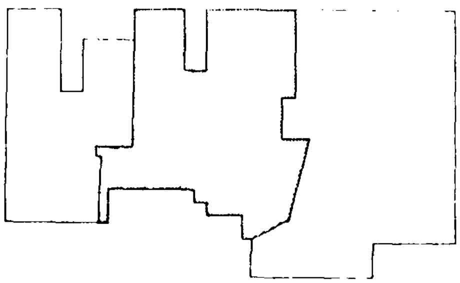


FIG. 6: SWATH ATTACK

REACTION TIME PERFORMANCE ANALYSIS

The major elements of the C^3 traffic within the MX system consists of three types of messages:

- Emergency action messages (EAMs).
- Retargeting messages.
- Status messages.

The priority of the message is as ordered above. The first two message types may be initiated by External Higher Authority (EXHA) and received by MX system gateway nodes for transmission into the MX wing in the MF simulcast network. Three types of gateway nodes are considered: those that interface with EXHA via HF links, those that interface via UHF links, and those that interface via the SLFCS.

Prioritized Access Control

Because of the large number of surviving nodes (about 125) and the number of hops required to cover the wing (4 or 5 hops), a terminal with a high priority message may incur unacceptable delay while waiting to make a reservation for channel access. For example, at a data rate of 600 bps, a reservation minislot of 15 bits will result in an average access delay of 6 seconds. To provide more rapid access for priority traffic, the priority reservation simulcast protocol was developed. The prioritized reservation frame is shown in Figure 7. As before, each missile station is assigned a reservation minislot, and each of these minislots is preceded by four minislots that are assigned to the Alternate Launch Control Centers (ALCCs) and the three gateway groups for priority transmission. For example, an EXHA message entering the MX network via the HF link is received by several or all of the HF gateway nodes. All nodes receiving the EXHA message will make a reservation simultaneously (group reservation) in the minislot corresponding to the HF gateway group. This is followed by simultaneous transmission of the message by each of the gateway nodes. Once channel access is gained by making a reservation, the message transmission follows in "blocks" of data. For example, the 4800-bit long retargeting message will be transmitted in six blocks of five messages, thus, providing an interrupt opportunity after each block.

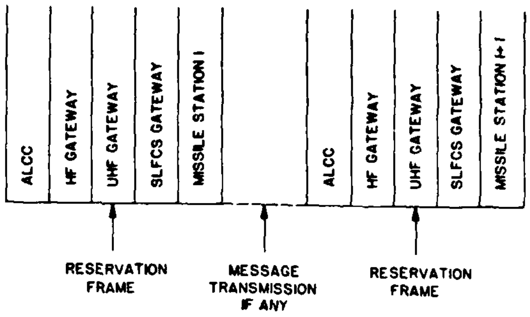


FIG. 7: PRIORITIZED RESERVATION FRAME

Reaction Time Estimates

The reaction time depends on the priority class of the message and the state of the network (busy or idle) when the message originates or enters the MX system. In general, reaction time is given by:

Reaction Time = Wait for Current Transmission Block to Finish
+ Reservation Time
+ Transmission Time
+ Delay due to Higher Priority Interrupts.

$$\text{Reservation Time} = \frac{15 \text{ bits}}{600 \text{ bps}} (4 \text{ hops})(5 \text{ minislots}) = 0.5 \text{ sec.}$$

$$\text{Transmission Time for a 600-bit Msg.} = \frac{600 \text{ bits}}{600 \text{ bps}} (4 \text{ hops}) = 4 \text{ sec.}$$

For example, an EAM message which arrives when the net is idle will have a reaction time equal to reservation time (.5 seconds) plus transmission time (4 seconds) which equals 4.5 seconds. If the EAM arrives when retargeting is in progress, the delay will have to include the transmission time for the data

block in transmission. Assuming a data block size of five messages, the average delay in this case will be 14.5 seconds which includes a 10 second access delay, 0.5 second reservation delay and 4 second transmission delay.

Summary of Reaction Time Analysis

The reaction time estimates developed for the different message types can be combined to give total system reaction time performance. Tables 2 through 4 can be used to obtain the system performance for various expected traffic scenarios. Table 5 exhibits the worst-case delay for the different message types, based on the following scenario: the retargeting message arrives while status collection is in progress, waits for the status message block to be complete, and gains access to the channel. The EAM arrives while the retargeting message is in transmission, waits for the current transmission block to finish, and gains access to the channel. When the EAM transmission is completed, the retargeting message transmission continues, and when this is finished, the status collection continues. For this traffic scenario, the worst-case cycle time (time for messages from all classes to complete transmission) is about 200 sec.

TABLE 2: EAM REACTION TIMES WITH DIFFERENT LOWER PRIORITY MESSAGES IN TRANSMISSION

Block Size	EAM Reaction Time: Mean (Sec)	EAM Reaction Time: Maximum (Sec)
600-bit retargeting or long status message in transmission		
1	6.5	8.5
5	14.5	24.5
10	24.5	44.5
150-bit status message in transmission		
1	5.0	5.5
5	7.0	9.5
10	9.5	14.5
30-bit short status message in transmission		
1	4.6	4.7
5	5.0	5.5
10	5.5	6.5

TABLE 3.A: RETARGETING MESSAGE REACTION TIME

Block Size for Transmitting Retargeting Message K	Number of Higher Priority (EAM) Messages Arriving during Retargeting Message Transmission, I: I = 0 Sec	I = 1 Sec	I = 2 Sec
K = 5	123.0	127.5	132.0
K = 10	121.5	126.0	130.5

Condition: Network idle at message initiation.

Retargeting message consists of 30 packets of 600 bits.

TABLE 3.B: RETARGETING MESSAGE REACTION TIME

Status Msg Size	Retargeting Msg Block Size K	Status Msg Block Size L = 1 (Sec) Mean Delay	L = 1 (Sec) Max Delay	L = 5 (Sec) Mean Delay	L = 5 (Sec) Max Delay
600 bits	K = 5	129.5	131.5	137.5	147.5
	K = 10	128.0	130.0	136.0	146.0
30 bits	K = 5	127.7	127.7	128.0	128.5
	K = 10	126.1	126.2	126.3	127.0

Condition: Network busy with status collection at message initiation, one EAM interruption before transmission is complete.

TABLE 4.A: STATUS MESSAGE REACTION TIME IN THE ABSENCE OF HIGHER PRIORITY MESSAGES

Status Msg Size	Status Msg Block Size, L: L = 1 (Sec)	L = 5 (Sec)	L = 10 (Sec)
600 bits	900	820	810
150 bits	300	220	210
30 bits	140	60	50

TABLE 4.B: STATUS MESSAGE REACTION TIME WITH ONE-HIGHER - PRIORITY (RETARGETING) INTERRUPTS

Status Msg Size	Status Msg Block Size, L: L = 1 (Sec)	L = 5 (Sec)	L = 10 (Sec)
600 bits	1,023	943	933
150 bits	423	343	333
30 bits	263	183	173

Retargeting message block size, K = 5

TABLE 5: WORST-CASE DELAY ESTIMATES FOR DIFFERENT MESSAGE TYPES

Status Msg Size	Retargeting Msg Block Size, K	Reaction Time (sec) EAM	Retargeting	Status
30 bits	K = 1	8.5	140.5	199.5
	K = 5	24.5	128.5	187.5
	K = 10	44.5	127.0	186.0

Status message block size, L = 5 (reservation slot for priority interrupt follows five status responses)

Table 5 shows an important relation between message block size and reaction time for the different message types. For example, when the retargeting message block size is decreased from 5 to 1, the EAM reaction time increases from 24.5 to 8.5 seconds. However, the retargeting message reaction time increases from 128.5 to 140.5 seconds because of the overhead introduced from the more frequent transmission of the reservation frames. Moreover, it appears desirable to keep the block size small, as long as the message rate is low. With the same example above, when the block size is decreased from 5 to 1 for the retargeting messages, the reaction time of an EAM message is reduced by roughly 70 percent, while the reaction time of the retargeting messages and status messages only increases by less than 10 percent.

The analysis was conducted on a parametric series of values and a prioritized reservation protocol. This protocol keeps the system in the reservation mode until a reservation is made. The system then goes to the message transmission mode until four hops have been completed, and then, if there are no more messages in the queue, reverts to the reservation mode.

The intent of this analysis was to show the effect on reaction time of various message types and various message lengths. The analysis technique applies to other message types and length and provides a useful tool for such analysis.

CONCLUSION

In this paper, we have described an MF simulcast radio system for the post attack MX C^3 system. Parametric performance estimates of survivability and reaction time are given based on simulation and analysis. These results indicate that simulcast is a viable option for providing a survivable and robust C^3 network, even for a rugged terrain deployment of the MX system. The multiple, simultaneous relay of a message can provide signal reinforcement needed to bridge across mountains or swath destruction. The broadcast routing associated with simulcast requires no control or monitoring overhead since all nodes act as relays. However, this requires strict control of traffic entering the network. This is done by imposing a prioritized reservation channel access control protocol. The single channel simulcast system described in this paper assumes a wing-wide access control discipline. Further improvements to the reaction time performance can be obtained by structuring a multichannel simulcast net. This can be done by partitioning the MX wing into regions (typically coincident with each squadron), and providing non-interfering simulcast nets for the command and control of each region. Gateway nodes will have to be provided for interregion communications, and this introduces greater complexity and control of the system.

ACKNOWLEDGEMENT

This work was performed under subcontract to the Boeing Aerospace Company, ICBM Division, MX Program Office, Seattle, Washington.

BIOGRAPHIES

NARAYAN SUBRAMANIAN

As a member of the technical staff of Network Analysis Corporation, Mr. Subramanian has had technical, management and supervisory responsibilities in the area of communications systems analysis.

Mr. Subramanian's involvement in military communications includes the analysis of both tactical and strategic systems. His current assignment is project manager for the development of NAC's Joint Tactical Information Distribution System (JTIDS) Simulation Model. This places him in the position of supervising and participating in the design of a complex software package which will be used to evaluate and select the network management and control techniques for this advanced tactical communications system.

Mr. Subramanian was project manager for C^3 studies on the MX missile system. He directed efforts to define alternative system configurations and protocols and to compare their performance, primarily survivabilitiy and response time. His supervisory responsibility includes the development of large-scale simulation models to evaluate performance of preferred system architectures.

For the Department of Energy, he developed specifications for an electronic instrusion detector system for the Los Alamos Scientific Laboratory and has defined a feasible network architecture to handle large-scale information transfer from several thousand sensors in a secure, real-time environment.

Before his association with Network Analysis Corporation, Mr. Subramanian was a Teaching Assistant and Fellow at Rensselaer Polytechnic Institute and a Teaching Assistant at St. John's University.

DR. IVAN T. FRISCH

One of the original founders of Network Analysis Corporation, Dr. Frisch is Senior Vice President and General Manager of New York Operations. He helped formulate and write the original program for the layout of the ARPA computer network. He has been responsible for testing broadcast packet radio signaling schemes for data transmission on coaxial cable systems and in the study of packet-switch architectures for high throughput systems. More recently, he has participated in the development of techniques for integrated voice and data traffic.

Dr. Frisch has been program manager for the modeling and analysis of the JTIDS (Joint Tactical Information Distributed System) program. He has also been program manager on a contract to Boeing Aerospace Corporation for the survivability and reaction time analysis for the communications for the proposed MX strategic weapon system. The project involves modeling of threat scenarios, system configuration, and performance analysis with the incorporation of evolving hardware, software and performance requirements.

Dr. Frisch directed the development of NAC's Computer CATV System Design Program, which represents one of the most complex and difficult applications of network analysis in existence. He has also directed projects in electronic funds transfer system, insurance communication systems and corporate communication systems for many commercial clients.

Before his association with NAC, Dr. Frisch was an associate professor of electrical engineering and computer science at the University of California, Berkeley. His professional background also includes a period as a Ford Foundation Resident as a member of the staff of Bell Telephone Laboratories. At Bell, Dr. Frisch wrote a computer program for the analysis and design of communication networks subject to station and link failure. The program was used for the design of new systems, the evaluation of the AUTOVON network, and the study of long-range communication network planning. This work served as a beginning for many subsequent studies on vulnerability and reliability.

Dr. Frisch was the founding Editor-in-Chief of Networks (John Wiley). He has written over 60 technical papers on all aspects of network analysis and design and is co-author of Communication, Transmission and Transportation Networks, Addison-Wesley, 1971, which won honorable mention in 1972 for the previous year's most significant contribution in the field of operations research.

Dr. Frisch has served on and chaired numerous IEEE committees and meetings and is a frequent speaker at national and international professional meetings. He is a member of the New York Academy of Science, a Guggenheim Fellow, and a Fellow of the IEEE.

Reference

1. West, Raymond H. and Taylor, Terry L., "A Simulcast Radio Relay System Model", International Conference on Communications, June 1980, pp. 12.5.1-5.

SYSTEM CONTROL FOR THE TACTICAL/STRATEGIC INTERFACE

Donald Spector & Senatro J. Iuorno
Rome Air Development Center
Griffiss Air Force Base, New York
William C. Kran & Robert L. Tufaner
Honeywell Avionics Division
St. Petersburg, Florida

ABSTRACT: The need for communications system control across the tactical/strategic boundary stems from the requirement to join tactical and strategic assets during periods of general or limited war, and in support of survival, recovery, and reconstitution efforts. Emerging control systems mirror the divergent technical advances in the systems they control, resulting in separate, different control hierarchies. This paper examines the cross boundary transactions required to provide interoperation and evaluates some potential solutions. The most promising developmental approach is to treat interoperability as a separate entity, centralized to the extent that survivability considerations permit; even though, ultimately, interoperability functions may be incorporated into other system control elements. An Interoperability Control Element (ICE) is proposed as a vehicle for further development and refinement of interactive system control techniques and procedures.

THE INTEROPERABILITY PROBLEM

Communications technology has made significant advances over the past twenty years. These advances have been incorporated into various communication upgrades within the Department of Defense. The strategic and tactical upgrades have occurred substantially independently of each other, with the result that the strategic and tactical communications worlds are finding interaction increasingly difficult. This deficiency in interoperability exists with respect to both the basic mission communications systems and with respect to the system control (SYSCON)

apparatus which is used to control and manage the mission systems. More impediments to interoperable SYSCON impend in the massive replacement of many manual SYSCON functions with data processing networks as embodied in the Tactical Communications Control Facilities (TCCF), Automated Technical Control (ATEC) Real Time Adaptive Control (RTAC) and the World Wide On Line System (WWOLS) upgrades. This substitution of machines which do not converse with each other, for people who speak a common language, will exacerbate tactical-strategic interoperability problems unless positive remedial action is taken.

As a means of gaining an improved understanding of the interoperability gap and of potential remedial measures, Rome Air Development Center initiated a study in January, 1979.(*) The study addresses three major task areas: a requirement evaluation task; a system control interoperability requirements and baseline definition task, and an equipment/software recommendation task. Work performed pursuant to the first two tasks, constitute the source material for this paper. (1)

CONTEXT OF SYSCON INTEROPERATION

In general terms three alternate management contexts may be hypothesized for interoperability system control purposes. These are:

1. Unified operation of the DCS and deployed tactical communications elements as a single integrated system.

2. Separate operation of the DCS and tactical networks with clearly delineated interfaces and a basic understanding by operators of each network of the resources and procedures available to the other.

(*) Information presented in this paper reflects work performed for Rome Air Development Center, Griffiss Air Force Base New York under contract to Honeywell Incorporated, Avionics Division, St. Petersburg, Florida. The contract number is F30602-79-C-0066.

3. Separate operation of the DCS and tactical networks with a rigid boundary and independent and different procedures.

The choice of the system control management concept clearly affects the amount and nature of information traversing the strategic-tactical interface.

In Alternative (1) the unified system control concept implies that a single system control activity maintains awareness of system status and directs control actions to maintain optimum overall system performance. To implement this control mode would require that unevaluated or partly evaluated data be forwarded to the control activity which would then formulate control directives as required to improve overall system performance.

In Alternative (2) the separate but mutually knowledgable control concept, strategic and tactical organizations would operate independently but with an exchange of information and requests for control actions. In this context one control organization would transfer information to the other whenever an actual or potential change in service across the interface is sensed. Control actions would probably not be requested per se. Rather an operational situation would be described which would cause the recipient to generate control actions in the context of his own system's resources and requirements.

In Alternative (3) the establishment of separate systems with a rigid, formal boundary would entail the least transfer of operational control data. Presumably the interfaces between the strategic and tactical systems would be preestablished by plan. Each system control organization thenceforth would concentrate its interoperability resources on verifying that its system is functioning to the boundary.

Interfacing of control systems requires a fundamental understanding of the hierarchical configuration

and operational capabilities of the systems to be interfaced. In the areas of tactical and strategic communications systems it is necessary to define the control infrastructures for both systems. The evolving strategic communications control system will consist of the familiar five level hierarchical structure of World, Theater, Sector, Node and Station. (2) (3) The operating elements of this structure will be supported by the WWOLS manual technical control facilities, orderwire structures and ATEC contingent on final procurement and deployment. Future strategic systems will result in major changes in the communications capabilities with the fielding of the on-going development programs including the Digital European Backbone (DEB) upgrade, AUTODIN II, AUTOVON Network Control upgrade, Secure Voice Improvement Program (SVIP) and the European Telephone System (ETS) program. System control of the DCS comprised of these new systems will follow the five level hierarchy with information flowing from the lowest level to the higher levels and control direction flowing down.

The evolving tactical communications control systems will consist of a mix of older tactical control concepts and equipments and the newer TRI-TAC equipments with a gradual phase over to TRI-TAC equipments and automated control concepts. In older tactical control concepts, information flows along communications paths through command hierarchies directly to respective service theater headquarters such as the Tactical Air Force Headquarters (TAF-HQ) and Corps Main for the Army. As deployments of Tactical Communications Control Facilities (TCCF) becomes a reality the system control functions will become aligned in accordance with the Communications System Planning Element (CSPE), Communications System Control Element (CSCE), Communications Nodal Control Element (CNCE) and Communications Equipment Support Element (CESE) equipment functions and hierarchical structure identified in the TRI-TAC system specification. (4)

Comparisons of the established strategic hierarchical control structure and the planned TCCF hierarchical control structure clearly illustrate that system level management configurations exist in each case; however, the two structures are different in functional terms because of the difference in mission requirements. No clear cut level of interoperability management practices can be stated simply by comparing the hierarchical configurations.

From a technical standpoint, TCCF and ATEC, the incipient tools of SYSCON, have different message repetoires, which are tailored to the equipment, nomenclature, and structure of the systems which they, respectively, support. These, too, differ far more than they coincide. An intermingling of strategic and tactical SYSCON is thus no straightforward melding of information; it is rather the establishment of a bridge between systems with different rules.

The incommensurability of tactical and strategic SYSCON structures and tools leads to the conclusion that the management context of a single, unified system (Alternative 1) is not feasible in the foreseeable future. A context somewhere between the separate but mutually knowledgeable (Alternative 2) and the separate with a rigid boundary (Alternative 3) is feasible. This situation was recognized early in the study, and thus became an underlying constraint upon the work which followed.

BASELINE SELECTION

In order to allow examination of tactical-strategic interactions in small, tractable units, a detailed methodology was employed. This methodology will be explained, along with summaries of the intermediate results. The flow of baseline selection activities is sketched in Figure 1, which should be consulted during the discussion which follows.

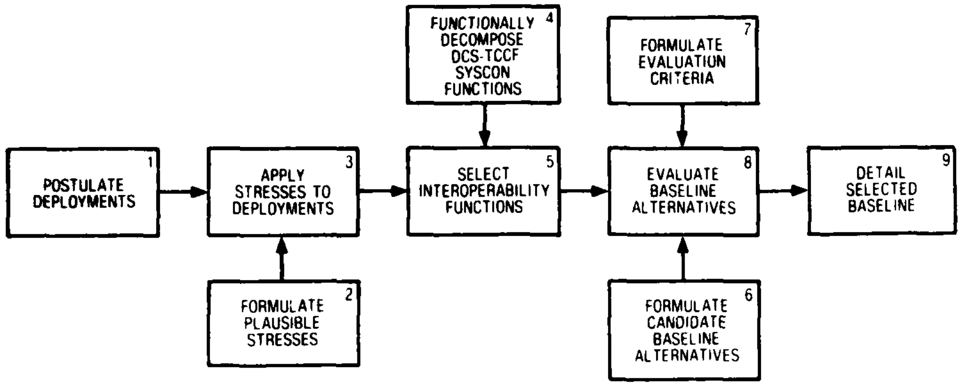


FIGURE 1 - BASELINE SELECTION METHODOLOGY

The first three steps consisted of the generation and mental exercising of scenarios entailing interoperation of tactical and strategic elements. In step 1 communications structures supporting hypothetical representative deployments were delineated. The deployments considered were a reconstitution of a destroyed DCS station with tactical equipment; deployment of a quick reaction force to an isolated corner of the world, and a joint U.S./Allied full scale deployment requiring tactical interfaces through the DCS.

The second step consisted of the formulation of representative stresses which might be imposed upon the communications configurations evolved in the first step. The set of stresses discussed ranged from normal operating nuisances to massive failures, and included a problem often overlooked: getting communications initially established and running.

Application of the stresses to the communications network, step 3, allowed tracing of the required SYSCON actions. From this, considerable detailed information was gained about the specific chain of actions required to respond to stress. This process of exercising the sample communications configuration was continued throughout the study and proved to be useful and practical.

In step 4 a considerable effort was necessary to identify what system control includes. Before interoperability system control could be identified it was essential to provide answers to questions such as: What is system control? What does system control include? What are the requirements for interoperability system control and how do they differ from day to day SYSCON? In order to answer these questions strategic rather than tactical system control was chosen as the subject for analysis aid for several reasons. First, the Defense Communications System (DCS) and its evolving control structure has been in existence since being created in the early 1960's from the parts of various military department owned systems. Secondly, the DCS or strategic system control structure, policy and procedures are well documented and standardized. In addition, the existing tactical system control structure and approaches found in both the Air Force and Army tactical programs are subsets of the strategic approaches; however definition and documentation varies by tactical O&M organization. The evolving TRI-TAC system will possess a control structure which contains the four hierarchical elements CSPE, CSCE, CNCE and CESE. Each of these four hierarchical elements have been assigned functional responsibilities and tasks. These are only generic assignments; detailed implementation

approaches and procedures have not yet been defined.

Analysis of the DCS system control identified a breakdown into six major functional areas as shown in the strategic SYSCON half of Figure 2. These functions are accomplished in varying degrees throughout the DCS. On the tactical side only those functions specified for the TCCF system could be equated to system control actions. The existing manual tactical technical control assets (i.e. TSC-62 and TSQ-84 vans) fall mainly into the patch and test category in response to detected problems or direction from higher level authority. Therefore, the interoperability system control task mainly addresses the interfacing of the TRI-TAC TCCF structure with the DCS control structure as shown in Figure 2.

Step 5 combined the results of scenario analysis, step 3, with the generic, detailed SYSCON analysis derived from step 4, for the purpose of deriving the functions involved in tactical-strategic interoperability. The analytical framework of steps 4 and 5 is shown in Figure 2. The figure shows the "Interoperability Control Element" (ICE) which, at this stage of analysis, formed a conceptual framework for study of interoperability requirements. (This conceptual ICE evolved into a tangible ICE, which will be discussed later). A detailed list of 36 interoperability functions was derived, which was refined into the ten functions listed in Table 1.

Selection of a baseline for implementation of the essential interoperability system control functions required the definition of implementation alternatives, step 6, formulation of the evaluation criteria, step 7, and evaluation of the alternatives based upon the selected criteria, step 8.

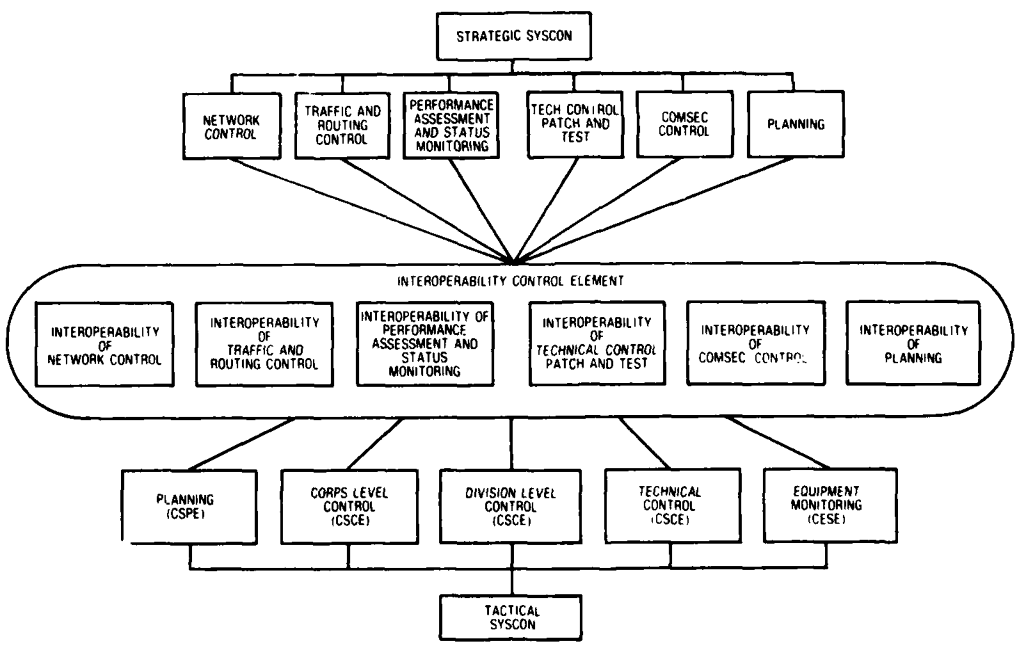


FIGURE 2 - INTEROPERABILITY CONTROL ELEMENT CONCEPT

TABLE 1 INTEROPERABILITY SYSCON FUNCTION LIST

1. Exchange of Switched Network Information (AUTOVON, AUTODIN, SVIP). This consolidated interoperability functional statement incorporates the functional requirements as follows:

   a. Exchange of network switch status
   b. Exchange of network configuration status
   c. Exchange of traffic statistics and loading information.
   d. Exchange of outage information. This item is also listed for other system activities in which outage information is exchanged.
   e. KAZCON information exchange.
   f. Network routing changes.
   g. Coordination of altroute activities and exchange of alternate routing information. This item is also stated under other circuit restoral activities which may require altrouting.
   h. Updates to switched systems routing tables.
   i. Exchange of contingency information pertaining to switched network operation or traffic loading.
   j. BSI and KDC status summary exchange.

2. Exchange of Dedicated Network Information.

3. Exchange of Circuit Outage Information. This function is additional to outage exchange information of the switched networks.

4. Fault Isolation Coordination. This function includes switched network F.I. activity and the exchange of user complaints.

5. Exchange of Quality Assurance Information. This function incorporates such items as performance assessment and circuit data exchange in support of quality assurance. It also includes the exchange of data to support F.I. and QA which relates to the QA portion.

6. Exchange of Satellite Information. Satellite status is considered here to be a procedural exchange which will follow the same reporting lines as link, equipment and configuration status.

7. Exchange of ECM and resulting ECCM Information.

8. Exchange of Planning Information. Planning information exchange includes but not limited to:

   a. C^3I Planning information exchange.
   b. System capacity information exchange for planning purposes.
   c. Crisis management information exchange.
   d. Planning coordination for mission support.

9. Exchange of Circuit Actions Information. This function includes all TSR/TSO activity and circuit updates normally included in circuit history files such as equipment alterations, user relocations, etc.

10. Exchange of General Information. This function is considered and required to insure unformatted and infrequent type requests for information are accommodated.

Baseline Candidates

Six levels of implementation capability/automation were identified which include varying degrees of man/machine interface from processor-to-processor direct exchanges to the manual techniques utilized in today's environment. The candidate baselines selected for study are as follows:

1. ATEC and TCCF system deployments offer an opportunity for processor-to-processor interfaces. Considerable modification to both ATEC and TCCF systems would be necessary to implement this approach. Each processor would be required to identify interoperability related problems in need of cross boundary coordination. Considerable software would be necessary to accomplish the interoperability fault recognition and isolation goal. This implementation alternative is identified as full implementation automated for future reference.

2. Impacts envisioned on ATEC and TCCF development systems give rise to a concept of implementation/automation which makes maximum use of the capabilities of ATEC and TCCF, but also places a tangible Interoperability Control Element (ICE) System between the appropriate hierarchical levels of TCCF and ATEC (or the FCO, in non-ATEC DCS environments) for the purpose of accomplishing interoperability systems control with minimum impact upon TCCF and ATEC. The ICE consists of a processor, CRT Terminal, printer, crypto units and modems and allows the ICE operator to access the ATEC, WWOLS and TCCF data bases. Processor assisted displays are used to reduce the clerical load upon the operators. This implementation approach is identified as full implementation semiautomated for future reference.

3. Another implementation approach, utilising only ATEC and TCCF equipments, is to assign the interoperability system control function to TCCF and ATEC operators. No ICE hardware is postulated. This concept provides processor assisted displays within ATEC and TCCF using their respective

terminals and processors as contrasted with the direct processor to processor interfaces of the full implementation candidate. Each interfacing sector (or FCO) and CSCE operator becomes responsible for the generation, protection and transmission of messages across the strategic/tactical boundary. Software additions to TCCF and ATEC would be necessary to accomplish this information exchange. This implementation alternative is identified as partial implementation automated for reference purposes.

4. This alternative is identical with the previous concept except that the exchange of information is accomplished manually by teletype or voice. This has the advantage of minimal impact on ATEC and TCCF systems since no additional software or displays are required. Therefore, the alternative is identified as partial implementation semiautomated.

5. All of the above implementation alternatives considered the appropriate hierarchical levels for information exchange which have been identified in the functional analysis. This option is the assignment of interoperability system control responsibilities at the lowest possible hierarchical levels such as switch-to-switch or station to station. Operators at various stations and switches are utilized to determine that a cross boundary problem exists and necessary information is exchanged manually by TTY or by voice. This alternative is identified as minimal implementation semiautomated for reference purposes.

6. The simplest nonimpacting implementation approach towards interoperability system control makes use of voice for cross boundary information exchange between operators at a strategic station and a CNCE or between operators at an AUTOVON switch and the tactical TTC-39 switch. Operators carry the burden of interoperability system control on an as needed basis. This alternative is identified as minimal implementation manual for reference purposes.

Baseline Selection Criteria

Baseline selection criteria utilized in evaluating the above six implementation alternatives are listed in Table 2. The actual baseline selection process involved comparing each of the baseline selection criteria against the six implementation alternatives for each of the ten interoperability system control functions in Table 1, and generating an annotated matrix of high, medium or low rankings. Upon completing the ranking matrix a sum of each level of goodness was obtained for each of the six implementation alternatives. The results of this analysis favored the full implementation semiautomated approach which was, therefore, selected as a baseline for further study and refinement during the last phase of the present contract.

TABLE 2-BASELINE SELECTION CRITERIA

1. Performance
   a. Response Timeliness
   b. Accuracy
   c. Low Data Base
   d. Usable Information Format
   e. Manual Override
2. Low Vulnerability
3. High Survivability
4. Security
5. Independent Control
6. Availability
7. Manning Intensity
8. Interoperability Mission Effectiveness
9. Impact on ATEC and TCCF
10. Low Documentation Needs
11. Manning Needs
    Percent Supervisor
    Percent Journeyman
    Percent Novice
    Percent Maintenance

Generic Attributes of Selected Baseline (ICE)

The selected baseline is the implementation alternative described as "full implementation, semi-automated". This alternative separates the interoperability SYSCON functions from the intra-DCS and intra-TCCF SYSCON, and concentrates them into a relatively small number of locations. Separate tools are used by separate personnel to pursue interoperability problems.

Although the detailed rationale for this choice is buried in the selection matrix, it is possible to generalize about the advantages of a separate, centralized ICE.

From a personnel standpoint, the interoperability functions are focused upon an individual, provided with processor assistance, who has the responsibility of providing liasion between the strategic networks and the upper echelon of the TCCF control structure. The differences in procedures and capabilities between the strategic and tactical systems suggests that the presence of an individual specifically charged with interoperability will facilitate smooth overall operation. Even though an understanding of how the tactical system operates could be expected to slowly permeate DCS personnel, the fluidity and changing configurations which can characterize a tactical deployment make maintenance of current tactical status very difficult if every individual who has some need for tactical information must stay updated. Centralization of ICE functions restricts the need for specialized knowledge and training to a relatively small cadre.

The selection of a tangibly separate ICE contradicts the conventional wisdom that hardware and software proliferation should be avoided and has been the subject of considerable debate. Nevertheless, in the current context of SYSCON development, it appears to be the logical course to follow, even though, consolidation of functions into existing SYSCON elements may be, in the abstract, desirable. As previously discussed, TCCF, ATEC, RTAC and WWOLS upgrades are being developed separately to fulfill the SYSCON requirements of the communications services which they support. Their continued evolution through engineering development, evaluation, and refinement into operational viability will be an extended process. Superposition of interoperability requirements upon these programs would likely result in further delays and uncertainties and the treatment of interoperability as another peripheral requirement. Separate ICE development is, therefore, recommended, and it should be noted, does not necessarily preclude ultimate functional integration into another SYSCON system if it is finally deemed desirable and feasible.

Adaptiveness or adaptability is a key and essential ingredient in the conceptualization and subsequent design of any system to support the plausible variations in interoperability requirements. The degree and variety [illegible] environment [illegible] subordinate or higher [illegible] functions have been lost, interrupted or isolated.

Paradoxically, the separate, relatively centralized ICE was determined to be at least equal to the other candidate approaches with respect to adaptability. The fundamental reason for this was that it enables the focusing of interoperability needs for a particular tactical deployment upon a relatively flexible

response to a particular situation, as contrasted with other alternatives which rely upon more data and procedures which are predispersed and consequently more difficult to alter.

INTEROPERABILITY CONTROL ELEMENT (ICE) DESCRIPTION

The ICE is defined at three separate levels, tied to the DCS SYSCON hierarchy:

Theatre Level ICE at ACOC
Sector ICE
Station ICE

These three ICE subsystems are described in the next three sections, followed by a short description of ICE communications.

Theatre Level ICE

Within the DCA theatre, several networks exist whose control is exercised from ACOC. These are the switched networks, AUTOVON and AUTODIN; terrestrial transmission system control exercised through ATEC; satellite transmission system control, RTAC; and strategic secure voice control. Additionally, dedicated special purpose networks exist whose network control may be exercised elsewhere, but whose interoperability aspects may be exercised through ACOC.

Within the tactical communications structure, this separation of functions is much less clearly defined due both to the integrated nature of TCCF system control equipment and to the fact that no operational experience with TRI-TAC equipment exists. However, in many cases, it is likely that the focal point of the tactical system will be at the CSCE operated by the signal brigade for Army deployments and at the TAF-HQ for Air Force deployments.

The ICE function at ACOC would therefore, on a day to day working basis, act as the interface between the semi-automated ACOC functions and the CSCE.

Generically, the sequence of actions involved in determining and resolving network or circuit types of interoperability performance degradations are shown in Figure 3. The sequence is shown originating in the DCS network; however had it been initiated in the tactical forces the process would be roughly the conjugate of that shown.

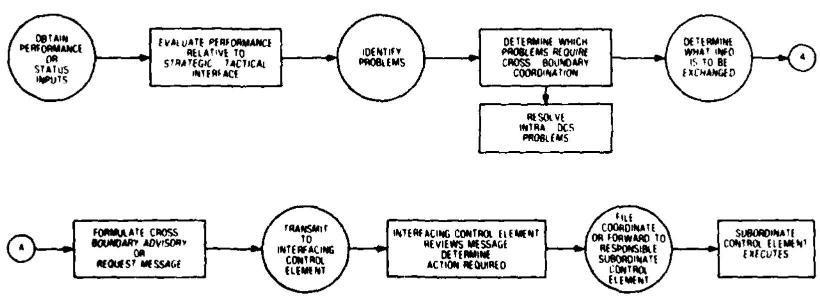


FIGURE 3 EXCHANGE OF CONTROL DATA FLOW PROCESS

The first three functions shown are part of the standard network or circuit performance evaluation process, and are performed by the organization charged with network or system control. Information describing performance of network elements is gathered using whatever automated or manual methods are available. This information is collated and evaluated in the context of the network as a whole. From this evaluation, problems are identified whose resolution could improve network service, or about which, using organization should be notified.

At this point, the interoperability aspects of the system control process begin to come into play. Network problems whose resolution can be assisted by actions from across the boundary are identified, as well as those which can be expected to degrade the service provided through the interface.

When a situation with cross boundary ramifications has been identified, the ICE function examines the situation in the light of the cross boundary constraints and formulates a request for control actions or notification of a situation. Some requests can be quite specific, such as a request for circuit switch destination code cancellation of traffic for a failed switch. Others may describe a problem, but leave the conjugate control organization the task of selecting the specific actions to be implemented in the light of its overall network objectives and resources. Requirements to restrict traffic flow for example would probably, in general, fall into this category since, usually they can be achieved through several means or combination of means.

Unique flow charts have been identified (1) which show the specialization of the generic network interoperability flows to AUTOVON, AUTODIN and dedicated networks, respectively.

Sector/FCO ICE

The Sector/FCO ICE performs three major functions:

1. Acts as a focal point for control, performance monitoring and fault isolation of portions of the terrestrial transmission system which connect with the tactical system from within the sector.

2. Provides security checking and message transfer between the strategic and tactical systems.

3. Provides facilities for assumption of ACOC ICE functions in case of loss or impairment of ACOC ICE.

The transmission system control function of Sector/FCO ICE provides a focal point for control of circuits and trunks traversing the strategic and tactical interface within the sector/FCO area. To provide this capability the ICE operator has access to the pertinent parts of the ATEC data base and can use ATEC capabilities (or FCO assets), subject to the direction of the Sector/FCO controller, for performance assessment, fault isolation, restoral, and other control actions. Requests for action toward the tactical side are directed to the appropriate CSCE who is responsible for selecting and implementing the appropriate control action.

A related subfunction, which is probably best performed by Sector/FCO ICE in some circumstances and ACOC ICE in other, is the interface control for dedicated networks. If the sector contains the interface and a substantial part of the network, the sector is probably a more appropriate location than ACOC.

The Sector/FCO ICE has the role of providing an interface between TCCF, which is accessed by AUTODIN, the ATEC message switching (or the FCO orderwires) system and the ICE operator.

Since the message switching capabilities of ATEC are not secure, all classified traffic is routed to the ICE operator, regardless of intended destination. Unclassified traffic destined for a DCS control element

other than the sector itself is converted to ATEC format and forwarded within the ATEC system utilizing ATEC as an interoperability system control message switch.

While the operation of ICE as a message interface, as has just been described, is an important part of its capability, the ICE operator is expected to play a significant role in the solution of interoperability problems. Most personnel in the DCS will know little about the tactical network, and vice versa. With ICE, interfacing responsibilities can be concentrated, and supported by message facilities and a data base related to interoperability. Thus the ICE operator can relatively rapidly build expertise and working knowledge pertinent to interoperability issues which would diffuse only slowly if responsibility were dispersed.

The third major function of sector/FCO ICE is to provide an alternate ACOC interoperability capability. For the designated sector/FCO ICE to be in hot standby, ready to assume ACOC functions rapidly, periodic data base updates would be sent from the ACOC ICE. The functions of sector/FCO ICE, when it has actually assumed the ACOC role, are, of course, the same as that described earlier for ACOC ICE.

Station ICE

The role of the ICE at the DCS station is very specific; to provide for coordination, performance assessment and fault isolation of cross-boundary circuits between the ATEC equipped DCS station and the interfacing tactical CNCE. These sites may be physically adjacent, or, more probably, one or a few tactical radio links may exist between the interfacing DCS station and the CNCE.

Cross-boundary circuits, except for secure voice, are 4 KHz analog channels. Circuits entering the tactical system will presumably be digitized into a 32 Kbps CVSD TRI-TAC channel for transmission to the CNCE, where the analog signal is reconstructed and available for monitoring. The reverse process occurs upon the circuit return leg, going from the CNCE to the strategic system. For secure voice, the Bellfield Seeley Interface (BSI) converts a number of encrypted 4 KHz analog channels into an encrypted TRI-TAC digital trunk group. This trunk group, and its constituent channels do not revert to analog form until finally decrypted and reconstituted at the user terminal. The BSI has a different set of interoperability system control needs, which are addressed in Volume II of a second interim report (5).

Since the digitization in the TRI-TAC system can possibly degrade complex high-speed modem signals, it is important that capability be provided to measure transmission parameters over these interfacing circuits. Modifications to the CNCE monitoring equipments are necessary since the Out of Service Test Set (OTS), which measures transmission parameters in ATEC, and the Manual Analog Tester (MAT), which is its CNCE counterpart, are not interoperable. Between the alternatives of placing a MAT at the DCS site or an OTS at the CNCE, the best choice is clearly the latter, since the OTS will be manufactured as a separate instrument whereas the MAT is an integral part of the CNCE. A Portable Controller Terminal Set (PCTS) is also necessary to facilitate control and provide hard copy output at the CNCE.

A direct data link between stations, with keyboard, VDU, and hard copy capability at each end would be desirable. However, since the internal functioning of the CNCE is such that messages may be lost in the teletype emulation mode of operation a voice orderwire is an acceptable and desirable alternative. This orderwire utilizes one of the digitized TRI-TAC channels and can be encrypted if the trunk encryption used in the radio links is deemed inadequate.

The three levels of ICE including Theatre Level ICE at ACOC, Sector ICE and Station ICE are shown in relationship to other system control

elements in Figure 4, ICE Operational Relationship to other SYSCON elements. As shown, ICE elements are resident at the ACOC, Sector/FCO and station levels. The heavy black line between the CNCE and the interfacing strategic station, CNCE and TTC-39 Switch represent mission circuits which cross the tactical-strategic boundary. The cross boundary circuits can terminate at different strategic stations which are under different sectors and nodes for control purposes. Since it

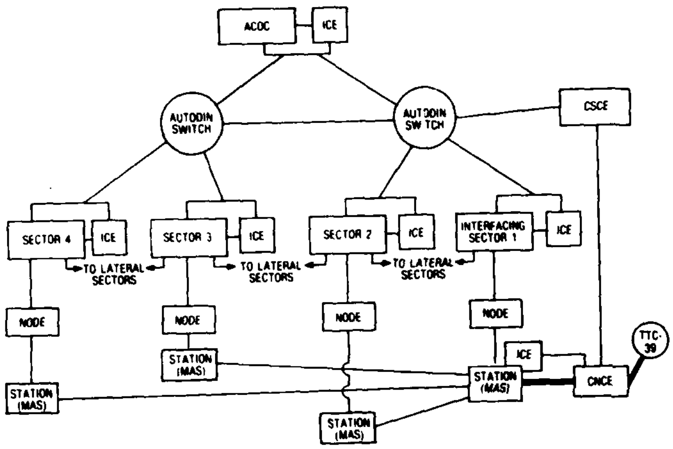


FIGURE 4 ICE OPERATIONAL RELATIONSHIPS TO OTHER SYSCON ELEMENTS

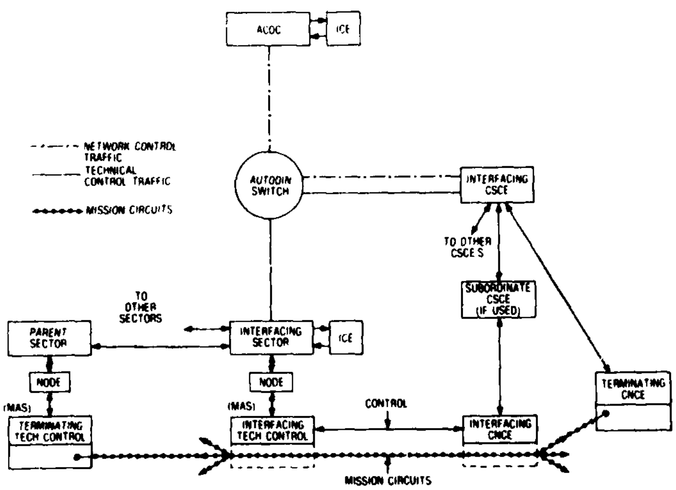


FIGURE 5 CONTROL INFORMATION FLOW

is highly unlikely that direct orderwire communications between all stations are available, the interfacing technical control and interfacing CNCE coordination allows the mission circuit interface to be controlled and fault isolated up to the strategic boundary by ATEC and across the boundary by the Station ICE capabilities. Figure 5, Control Information Flow, illustrates the control interface possibilities. It shows three levels of control and their interfaces. These include the control level between the interfacing strategic station and CNCE, the coordination and control information flow between the interfacing CNCE (or terminating CNCE's) and the distant end terminating strategic stations and the level of interface between the theatre ACOC and the interfacing CSCE for network control purposes.

SUMMARY

The differing paths of evolution of tactical and strategic SYSCON have led to systems whose elements will have difficulty interacting with each other. Analysis of cross-boundary transactions has definitized the functions which must be implemented to improve tactical/strategic compatibility. The most promising developmental approach is to treat interoperability as a separate entity, centralized to the extent that survivability considerations permit; even though, ultimately, interoperability functions may be incorporated into other system control elements. An Interoperability Control Element (ICE) is proposed as a vehicle for further development and refinement of interactive system control techniques and procedures.

REFERENCES

1. System Control for the Tactical/ Strategic Interface and the Secure Voice Improvement Program - Second Interim Report, Volume I - Baseline Selection; 9 July 1980. Generated under RADC Contract F30602-79-C-0066.

2. DCA Circular 300-50-6 Systems Control of the Defense Communications System; 24 June 1977.

3. DCA Circular 310-50-5 DCA Operations Control Complex and Operational Direction over the Defense Communications System; 9 November, 1977.

4. Performance Specification for the Communications System Control Element (CSCE) of the Tactical Communications Control Facilities (TCCF) - (Communications Control Center AN/TYQ-16 ( ) (V)) - Appendix 10, Concept of Operations of Tactical Communications Control Facilities in the Management and Control of Tactical Communications, Spec. No. TTB1-3001-0011; 31 December 1974 updated to SCN-07; 2 June 1977.

5. System Control for the Tactical/ Strategic Interface and the Secure Voice Improvement Program - Second Interim Report - Volume II, Secure Voice Improvement Program (SVIP) (U) CONFIDENTIAL - 9 July 1980. Generated under RADC Contract F30602-79-C-0066.

BIOGRAPHY. Donald Spector is Project Manager of the System Control Program at Rome Air Development Center, Griffiss AFB N.Y. This program is concerned with the monitoring of performance of major analog and digital communications systems. Information from this program is used in the planning and redistribution of communications assets to provide for optimum capacity under changing military conditions.

Since joining RADC in 1961 Mr. Spector has been involved with antenna design both in the UHF and HF portions of the spectrum. From 1962 to 1963 he worked in the area of of extended range air-to-ground communications involving ionospheric tropospheric scatter. From 1963 to 1966 he worked on the design of a survivable command and control communication system. From 1966 to 1976 Mr. Spector served as group leader of a Multiplex group where he managed the development of the first asynchronous time division multiplexer equipment used in the Defense Communications System. He further directed research and development efforts which enhanced performance of high speed digital systems operating in a highly unstable propagation media.

Mr. Spector received a B.S. Degree in Physics from the College of the City of New York in 1961 and a Master of Science and Systems Management from the University of Southern California in 1971. He has authored papers in the areas of digital multiplex design, survivable communications and system control. Mr. Spector is a member of the Institute of Electrical and Electronics Engineers and past chairman of the Rome Chapter of the IEEE Communications Society. He is also a member of the Armed Forces Communications Electronics Association.

BIOGRAPHY. Senatro J. Iuorno is a Project Engineer in the Rome Air Development Center Communication and Control Division, Griffiss AFB, N.Y. He is currently involved in the development of system control techniques for application to analog and digital communications systems and is the Laboratory Contract Manager for the contract which resulted in this paper. Since joining RADC in 1955 he spent eight years in the development of electromagnetic intelligence data processing techniques. In 1963 he moved into the Communication and Control Division where he has been involved in the design and development of message and voice switching systems, communications interface equipment and Automated Technical Control (ATEC) equipment.

Mr. Iuorno received a B.A. Degree in Physics from Syracuse University in 1955. He is a member of the Institute of Electrical and Electronics Engineers and also a member of the Armed Forces Communications Electronics Association.

BIOGRAPHY. Robert L. Tufaner is a Senior Systems Engineer with Honeywell Avionics Division in St. Petersburg, Florida. Since joining Honeywell in May 1976, he has been involved in systems engineering, analysis and requirements definition efforts supporting the prototype ATEC development effort; the digital application of ATEC study and development effort; and the "ECCM Aspects of System Control" study for the Rome Air Development Center. He also contributed to internal studies attacking the man-machine interface problem in high stress technical control environment. Mr. Tufaner is currently involved in the system engineering, analysis and definition efforts for the RADC study which addresses "System Control for the Tactical/Strategic Interface and Secure Voice Improvement Program".

Before joining Honeywell, Mr. Tufaner spent twenty years with the United States Air Force in numerous tactical and strategic communications maintenance and technical control positions. Prior to joining Honeywell, he was Superintendent of the Transmission System Division, Systems Evaluation Directorate, Air Force Communications Service. He achieved his GEC National Certificate in Mathematics at Dover England in 1961. Mr. Tufaner has written and presented several treatise on performance monitoring and assessment of communications systems and networks.

BIOGRAPHY. William C. Kran is a Staff Engineer with Honeywell Avionics Division in St. Petersburg, Florida. Since joining Honeywell in January 1972, he has been involved in lead engineer hardware design for the initial ATEC development program and was part of the field test team in Germany during the ATEC evaluation program. Mr. Kran was a task leader responsible for various phases of an RADC sponsored study "ECCM Aspects of DCS System Control" and is presently Technical Director of a two year RADC sponsored study "System Control for the Tactical/Strategic Interface and Secure Voice Improvement Program".

Mr. Kran was previously a Senior Engineer with Collins Radio Company, where he was involved with the design and development of a mini computer controlled Communications Link Analyzer (CLA-101) system for commercial use by AT&T.

Mr. Kran received a diploma from DeVry Technical Institute in 1955, a BSEE from the University of Illinois in 1962 and completed numerous graduate level courses at the University of Santa Clara and Iowa State University.

TACTICAL CIRCUIT SWITCHED NETWORK CONTROL*

Yau-Wu Tang
The MITRE Corporation
Bedford, Massachusetts

ABSTRACT: This paper systematically analyzes the performance of a circuit-switched network. Based on these analytical results, the concepts and algorithms of switched network monitoring and control functions are derived. The material presented in this paper represents theoretical results, and requires further validation.

I. INTRODUCTION

The tactical circuit switch network monitoring and control function is one of the major responsibilities for maintaining a highly dynamic tactical communication network. It includes the following functions:

1. Monitoring network performance. Network traffic data, equipment status, trend data and out-of-tolerance alarms are monitored.
2. Monitoring equipment faults as related to internodal switched trunk connectivity.
3. Detecting malfunctions of the circuit switch and trunk groups using statistical traffic data.
4. Correlating the faults detected in items 2 and 3 above with the impact (anticipated or actual) on traffic load between nodal switch pairs.
5. Controlling the switched network, including analysis to determine recommended alternatives and

* The work reported in this paper was performed under USAF Contract No. F19628-80-C-0001.

validation and implementation of control actions.

The tactical switched network is a meshed network. Each switching center will have trunk groups connected to several adjacent switching centers. Each switching center is also the center of a star network with several small switches connected to it. The switching equipment at the switching center is a processor-controlled analog/digital hybrid tactical switch which could be used for local as well as tandem traffic. The originating office control concepts are used in the routing selection algorithm. This means that one primary route and several alternate routes may be chosen at the call originating switch for establishing a path between two switching centers.

In this paper the properties of a tactical circuit switched network are systematically analyzed. Based on the analytical results, the concepts and algorithms for switched network monitoring, fault detection and correlation and control action initiation, validation and implementation are developed.

II. NETWORK ANALYSIS

In this section the properties of a tactical circuit-switched network are analyzed, and the relationships among circuit switches, trunk groups and network performance are discussed.

1. Overall Performance Analysis

Calls within a circuit switch may be blocked because of the unavailability of switching equipment, such as signalling/supervision equipment and the switching matrix. Calls from one switch to another may also be blocked because of the unavailability of the trunking equipment. The node-to-node grade-of-service (NNGOS) matrix, which represents the performance of the switched network, is defined as the blocking probability of a call originating from one switch node and terminating at another switch node. For a network with n nodes, the NNGOS can be represented as an n x n matrix. The overall network performance can also be represented by the network performance value (np-value), which is defined as:

$$np = \sum_{i} e^{-k X_i}$$

over all nodal pairs

in which X_i is the NNGOS of i th switch nodal pair and k is the network performance characteristic constant. The network performance is maximized when the np-value is minimized. The network performance characteristic constant k determines how much improvement in nodal pairs with extra low NNGOS should be emphasized.

The NNGOS is a function of the switch and trunk group throughput. Switch throughput can be represented by the circuit switch grade-of-service (CSGOS), which is the blocking probability of a circuit switch. Trunk group throughput can be represented by the trunk group grade-of-service (TGGOS), which is the blocking probability of a trunk group. To relate the CSGOS and TGGOS to the NNGOS, the characteristics of a tactical circuit-switched network should be examined. For such a network a finite number of different routes may be used to complete a call from one switch node to another. Each route may involve one or more trunk groups and two or more circuit switches (figure 1). If the blocking probabilities for each switch and each trunk group are given, the blocking probability of each route can be calculated using probability theories. Consequently, the probability of a call being blocked by all possible routes can also be calculated. The mathematical details are described in reference 1. The main point is that NNGOS can be calculated if CSGOS and TGGOS are properly measured.

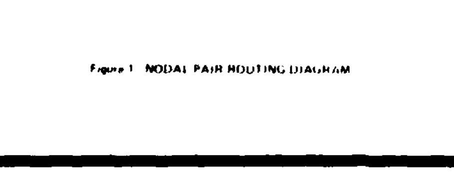


Figure 1 NODAL PAIR ROUTING DIAGRAM

The impact of call preemption on NNGOS should also be considered. The preemption feature in a tactical switched network does not increase the network throughput; it merely replaces existing calls with higher-precedence calls. However, excessive preemption within a network may increase the average call setup time and, in consequence, also increase the switch and trunk group load, especially on the signaling/supervision equipments. Subscribers whose calls are preempted will most likely try to reestablish the connection by reinitiating the call; this will also impose an extra load on the switched network.

2. Circuit Switch Performance Analysis

Circuit switch performance can be represented by circuit switch grade-of-service (CSGOS), which is the probability of call blockage because the switch is unable to complete a call. Calls will not be counted as switch blockage if they were blocked because of factors outside the switch, such as the called party being busy or failure to find an available trunk. Switch blockage could be due to lack of signaling and supervision equipment or lack of equipment to complete a path. The calculation of blocking probability due to lack of signaling and supervision equipment is very complicated because:

A. Different types of signaling/supervision equipment are used for different types of telephones and terminals.

B. In the case of signaling/supervision equipment being busy or having failed, different responses may be provided for different types of calls.

The overall probability that a call is blocked because of the unavailability of the signaling/supervision equipment could be done by measuring the number of calls N_1 which complete the signaling/supervision procedures (including the calls with illegal digits and called party busy) and the number of calls N_2 which fail the signaling/supervision procedures. The signaling/supervision blocking probability P_s can be calculated as:

$$P_s = N_2/(N_1 + N_2)$$

After completion of signaling/supervision procedures, the switch determines the inlet and outlet terminals and the common equipment for completing the path. The space division matrix (SDMX) or time division matrix (TDMX) connects the inlet terminal to the outlet terminal to form a path. In case common equipments are needed, the SDMX or TDMX connects the inlet terminal to the common equipment and then connects the common equipment to the outlet terminal. Overloaded SDMX or common equipments, or malfunction of SDMX, TDMX or common equipments, may affect the CSGOS.

The probability of failure to complete a path for calls whose inlet and outlet terminals have been determined should be measured as follows: The number of calls N_3 with inlet and outlet terminals determined and the number of calls N_4 with the path between inlet and outlet terminals established should be measured. The blocking probability P_f can be calculated as:

$$P_f = 1 - N_4/N_3$$

The overall switch blocking probability (CSGOS) can be calculated as:

$$CSGOS = P_s + (1 - P_s)\, P_f$$

3. Trunk Group Performance Analysis

Trunk group performance can be represented by the trunk group grade-of-service (TGGOS), which is the probability that the trunk group will fail to provide an idle trunk to complete a call. TGGOS can be obtained by measuring the number of call attempts to find an idle trunk from a trunk group T_1 and the number of calls for which there is no available idle trunk T_2 because all trunks are in use or the trunk group load limit would be exceeded. TGGOS is the ratio of T_2 and T_1, that is:

$$TGGOS = T_2/T_1$$

Since the trunk group load control limits depend on call precedence, the trunk group blocking probability is also call precedence-dependent. In other words, TGGOS should be measured for every trunk group and every call precedence.

4. Preemption Analysis

The probability of a call being preempted because the switch resource has to be reallocated to a higher precedence level should be measured as follows:

A. Measure the total number of calls established at each precedence level N_5 in a switch. A call is considered as established if the full path between the calling party and the called party is established; that is, the called party receives and responds to the call.

B. Measure the total number of calls (at each precedence level) preempted because the switch equipment has to be preempted for a higher-precedence-level call N_6.

C. The ratio of item B to item A represents the probability that a call at a given precedence level may be preempted. This probability should be calculated for each precedence level.

The probability of a trunk at a given precedence level being preempted by a higher-precedence-level call can be calculated as follows:

A. Obtain the number of attempts T_3 to find a preemptable trunk at a given precedence level. The data should be taken for each precedence level to be preempted, that is, the data should be taken separately for attempts to preempt a trunk which is busy at the routine level (routine trunk), priority level, immediate level and flash level. Only the precedence level of the trunk to be preempted is considered, not the precedence of the preempting call.

B. Obtain the number of times an attempt to find a preemptable trunk is successful, T_4. The data is taken as described in item A.

C. The probability of attempting to preempt a trunk at the precedence of interest is equal to the ratio of item A at that precedence to the number of idle searches (i.e., T_3/T_1).

D. The probability of a trunk being preempted at the precedence of interest is equal to the ratio of item B at that precedence to the number of idle searches (i.e., T_4/T_1).

5. Traffic Load Measurement

The traffic intensity represents the traffic load offered to or carried by a switch, a trunk group or other switching equipments. The traffic intensity expressed in erlangs represents the average number of calls carried simultaneously over a period of one hour. The average number of calls carried can be measured by periodically sampling the number of calls carried at the switch and trunk group.

The actual offered traffic intensity cannot be measured directly because the call duration of blocked traffic cannot be measured, and the blocked calls may be reinitiated. If one neglects the radial effect and assumes the average call duration for the established call is the same as for the blocked call, then the offered traffic intensity is equal to the carried traffic intensity multiplied by the ratio of the number of calls offered to the number of calls carried.

6. Traffic Source Analysis

The traffic source for switches and trunk groups is the amount of node-to-node traffic contributing to the switch and trunk, and can be obtained using a combination of direct measurement and analytical method. The traffic source information serves as the basis for determining the network control action.

The Traffic Source for a Switch. The traffic load on a switch can be divided into four categories, as follows:

A. Local loop traffic.
B. Tandem traffic.
C. Local loop to remote traffic.
D. Remote to local loop traffic.

All these data can be reported directly at the switch of interest using the measurement algorithm described in section II.5.

The following information is useful:

A. Total traffic load on the switch. This data can be used by the network controller to determine if the switch is overloaded.

B. Percentage of local traffic, tandem traffic, remote traffic originated locally and remote traffic terminated locally. These data represent the switch usage distribution. In case of switch overload or malfunction, the network controller could use the switch load distribution to determine the proper control actions (see section III.4).

The Traffic Source for a Trunk Group. The traffic source of trunk group traffic cannot be measured directly, but can be obtained analytically using the element grade-of-service (CSGOS, TGGOS, and NNGOS) and the measured node-to-node traffic load. The analytical method can be summarized as follows:

A. For each node-to-node traffic pair, use the analytical method described in reference 1 to calculate the traffic load on the trunk group of interest.

B. Repeat step A for all node-to-node traffic pairs and record their traffic load on the trunk group of interest.

III. SYSTEM MONITORING AND CONTROL

1. Traffic Data Trends and Traffic Alarms

As discussed in the previous section, the performance of each individual element (such as switches and trunk groups) will affect the overall performance of the switched network. In order to prevent the occurrence of serious problems in the network, the performance of each individual element and the network as a whole should be monitored. The trends of these data should be analyzed to predict any potential trouble. In summary, the following data should be monitored:

Circuit Switch Grade-of-Service (CSGOS).
Traffic Load on Circuit Switches.
Probabilities of calls being preempted at a switch.
Trunk Group Grade-of-Service (TGGOS).
Traffic Load on Trunk Groups.
Probabilities of calls being preempted at a trunk group.
Node-to-Node Traffic Load.
Node-to-Node Grade-of-Service (NNGOS).

For each datum of interest, short-term data and long-term data should be maintained. Short-term data are used to detect sudden performance changes, while long-term data are used to detect slow changes.

For each datum of interest, two types of alarms may be used to monitor the changes of the data: threshold and tendency alarms. The threshold alarm is set if one or more data points exceed the preset alarm threshold. The tendency alarm is set if the data exceeds a lower-level threshold with a slope greater than a prespecified value. For both threshold and tendency alarms, the statistical uncertainty should be considered. This can be done by setting the alarms only if the received data exceeds the threshold by more than two or three standard deviations of the statistical uncertainty.

2. Fault Detection

The faults to be discussed fall into three categories:

A. Equipment Faults - The malfunctions of the switching and transmission equipment are defined as "equipment faults". They include switch and trunk group malfunctions.

B. Estimation Faults - Estimation errors made in predicting the traffic load between the nodal pairs are considered as "estimation faults".

C. Indirect Faults - Faults that are caused by equipment faults and/or estimation faults are defined as "indirect faults", including:

Switch Overload
Trunk Group Overload
Degraded Switch Efficiency
Degraded Trunk Group Efficiency

The equipment faults are normally detected electronically. Analysis of the equipment status reports will identify the malfunctioning switch/trunk group and its effects on the switch/trunk. The equipment faults may also be detected using the traffic data.

When the configuration remains unchanged, the element grade-of-service is a function of traffic load and can be calculated analytically or predicted empirically (figure 2). When the element is in normal condition, the scatter plot of measured CSGOS and TGGOS vs. measured traffic load should coincide with the predicted curves illustrated in figure 2a. If equipment failure occurs, the measured CSGOS and TGGOS will be consistently higher than the predicted value illustrated in figure 2b. The standard deviation of the difference between the measured and predicted value can be calculated as:

$$D = (E_m - E_t) / \Delta E_m$$

in which E_m is the measured CSGOS/TGGOS, E_t is the predicted value and ΔE_m is the statistical uncertainty of the measurement. If the trend of the standard deviation is toward negative values, as illustrated in figure 3, it is an indication of equipment malfunction.

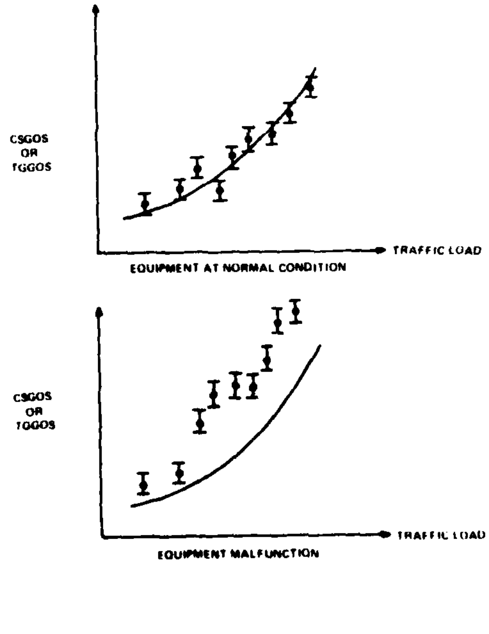


Figure 2 ILLUSTRATION OF FAULT DETECTION

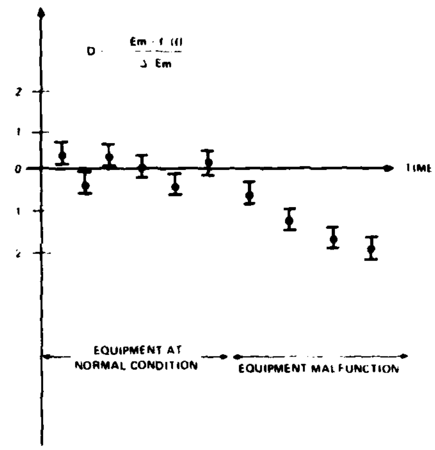


Figure 3 NUMBER OF STANDARD DEVIATION DIFFERENCE VS TIME

3. Fault Correlation

When the equipment or estimation fault occurs, the switch, trunk groups and node-to-node grade-of-service within the network will be affected. The NNGOS algorithms, described in reference 1, can be used to calculate the new TGGOS, CSGOS and NNGOS values based on the new switch/trunk group configuration and traffic load estimation. The calculated grade-of-service must agree with the measured value (within the statistical uncertainty), otherwise some equipment or estimation faults may not be identified.

4. Network Control

The objective of switched-network control is to provide and maintain required communication capability among all circuit-switched subscribers. When a part or all of a network is in an abnormal condition, various types of traffic controls may be needed to improve the network performance or to maintain communication capability for essential subscribers. When a group of faults are detected, the network performance value and NNGOS matrix should be calculated and examined, and the impact to the network performance should be determined. If the network performance is within tolerance, no immediate control action is required.

If a portion of the network is affected, control action should be taken to route traffic around the trouble area. The following control actions may be implemented:

1. Directionalization of trunk groups. This prohibits the switch at one end of the trunk group from seizing the trunk, i.e., only one switch is allowed to propagate the call through the trunk group. The switch at the other side of the trunk group is forced to use alternate routes.

2. Add or delete alternate routes. Overloaded trunk groups or switches should not be used as alternate routes, while low load trunk groups could be used as alternate routes for the low-grade-of-service ~~switch~~ pairs.
3. Routing table changes. The primary and alternate routes may be modified to redistribute traffic load. Also routing tables may be changed to avoid nodal isolation if a switch or a trunk group is totally out of service.

If the network traffic cannot be routed around the trouble area, or if the network's overall load is too high, then certain control actions may be taken to limit some subscribers' access to certain switches or trunk groups. To determine the control action, the traffic source that causes the network overload should be determined (see previous section).

If the major traffic load is originating from a single switch, the trunk group access control should be applied. Each subscriber is class-marked for limited trunk group access by a trunk group access control level. When one of the control levels is imposed on the switch, all subscribers with that control level will be prohibited from accessing any trunk groups.

If the major traffic sources are calls focused toward a particular switch, zone restrictions may be applied to other switches to reduce calls to the trouble switch. Subsets of subscribers within a switch can be class-marked using sets of zone restrictions. Each of these sets of restrictions will prohibit the terminal from completing a call to a certain area code, switch code or group of area/switch codes.

If the traffic overload occurs on local loop traffic, the switch access control should be applied. Each subscriber is class-marked for limited switch access by switch access control levels. When one of the control levels is imposed on the switch, all subscribers with the same control level will be prohibited from accessing the switch.

If the preemptions occur too often, the trunk group load control should be applied. Each trunk group has limitations on maximum numbers allowed for calls at or below a given precedence level. That is, within the trunk group, only a smaller number of trunks is allowed for the lower precedence calls.

The intended control action can be validated before it is implemented, using either or both of the following methods:

Analytical Method. The effect on traffic load because of zone restriction or switch level control can be predicted analytically. The availability of trunk groups and switches can also be ascertained (including the effect of trunk group load control and the effect of equipment malfunction). The NNGOS of all nodal pairs can be calculated using the measured traffic load, trunk group and switch availability and the new routing tables. If the calculated NNGOS is still out of tolerance, the control action should be reexamined.

Simulation Method. Network behavior can be predicted using the simulation technique. The traffic load among the nodal pairs can be calculated using the measured data, adjusting for zone restriction and level control. The network capacity (that is, the availability of the trunk groups and switches) can be determined using the analysis described throughout this paper. With the above initial data, the simulation program should create the traffic among the nodal pairs and process this traffic to determine the NNGOS. The simulation technique should be similar to that described in reference 2. Only the key factors in the network, such as routing selection, should be simulated. The usefulness of the simulation method will depend on the size of the simulation program and the simulation time necessary to validate a control action.

IV. PROCESSOR AIDED NETWORK CONTROL AND MAN-MACHINE INTERFACE.

The complex algorithm for calculating the network performance parameter, the continuous monitoring of the network

performance, and the complicated control decision and impact study all suggest that a processor is needed to aid the network controller to perform the network control function. The decision and control procedures from reception of data to control implementation can be subdivided into five steps:

1. Data Base Update - Forming statistical and status data (histograms) from raw data.
2. Trend Alarms and Status Alarms - Using statistical data and status data to derive trend alarms and status alarms.
3. Fault Detection - Using statistical data and alarms to determine faults.
4. Fault Correlation - Correlating equipment/estimation fault with indirect faults.
5. Control Action - Based on the faults, determining and implementing control action.

This section identifies the functions which can be done by the processor and the controller. The basic concept is that the processor will be a tool to assist the controller to perform the network control function. The controller will be the driver for all control actions.

1. Data Base Update - Interface between the processor and switching equipment should be provided such that the traffic statistical data and equipment status data is received at the processor electronically. Reception of data, trend histogram updating and status data updating should be done by the processor without manual assistance. However, the data should be made available to the controller for manual analysis.

2. Alarm Processing - The controller should decide which trend histograms or status data are to be analyzed automatically by the processor. The processor should analyze these data, using the algorithms given in previous sections, and determine the trend and status alarms. All histograms and status data should also be provided to the controller for possible manual decision about alarms. The processor should manage both processor and manually determined alarms so that all alarms may be coordinated and presented to the controller for further processing.

3. Fault Detection and Correlation - The algorithms given in Sections III.2 and III.3 may be implemented in the processor for automated fault detection and correlation. The automated fault detection function includes equipment fault detection based on the status data, equipment fault detection based on the traffic statistical data and estimation fault detection based on traffic statistical data, such as the node-to-node traffic load, the switch traffic load and the trunk group traffic load. The automated correlation function verifies that the switch load, the switch grade-of-service, the trunk group load and the trunk group grade-of-service match the calculated value based on the node-to-node traffic load.

   Because of the complexity of the switched network, some faults may not be detected or correlated automatically. The processor should provide network information to the controller for possible manual fault detection and correlation. The following information is useful:

   a. Trend histogram and equipment status data.
   b. Traffic source on trunk group and switch.
   c. Preemption related information.
   d. Traffic load distribution among the alternate routes.

4. Control Action Initiation and Implementation - The switched-network control principle, as stated in Section III.4, may be implemented in the processor for automated generation of control action. The generated control action should be treated as the "recommended action" and must be subject to the approval of the network controller. The processor should also provide the capability to accept the controller-determined control action or modification to the processor-suggested actions. The control action validation algorithms, as stated in Section III.4, may also be implemented in the processor for validating both processor-suggested or manually determined actions. The control action validation should be an

optional procedure to be initiated by the controller. Upon the approval of the controller, the processor should be capable of distributing the control action to the affected circuit switches and monitoring the implementation of the control actions.

V. CONCLUSION

This paper provides algorithms for switched network monitoring and control. It shows that network parameters can be analyzed analytically, and that the network control action can be derived based on these analytical results. However, if this concept is to be implemented, the following work must be done:

1. All algorithms must be verified using the simulation technique. A simulation model has been developed, and test results indicate that the basic mathematical model is correct. Reference 2 gives the simulation results.

2. The required ability of the network controller must be analyzed. As described in section IV, the processor should only be used as a tool to assist the controller to perform the required function. The controller must understand the switched-network principle, the available parameters and the impact on the control action.

3. The tactical switching equipment must be modified such that processes may communicate electronically as stated in section IV.1.

REFERENCES

1. Y. W. Tang and L. J. Elterman, "Performance Analysis and Routing Table Generation for Tactical Switched Network," NTC'80.

2. L. J. Elterman and Y. W. Tang, "Tactical Switched Network and Test Results," NTC'80.

BIOGRAPHY

Yau-Wu Tang is a Technical Staff Member of The MITRE Corporation. Since joining the MITRE staff in July 1977, he has been involved in developing the algorithms for circuit switched network routing table generation and network performance parameter monitoring, and is presently developing the concept and specification for tactical communication network control.

Yau-Wu was previously a Research Engineer for GTE Sylvania at Needham, Mass., where he worked on the tactical circuit switch development and the Minuteman Launch Control Facility Simulation. He was also a Research Associate at Purdue University and at Northeastern University, where he worked on experimental high energy physics research.

Yau-Wu holds a Bachelor's degree in Physics from the National Taiwan Normal University, and a Master's degree and Ph.D. Degree in Physics from Northeastern University, Boston, Mass.

SYSTEMS CONTROL IN TACTICAL DIGITAL COMMUNICATIONS SYSTEMS: A STUDY IN DISTRIBUTED CONTROL

LTC James A. MacStravic
Joint Tactical Communications Office
Fort Monmouth, New Jersey

ABSTRACT: Tactical communications systems must be survivable, flexible, reliable and meet the mobility requirements of the users of the system. These characteristics become more important in the digital communications systems of the future. The control structure of these communications systems must effectively support these characteristics.

In 1973, the Joint Chiefs of Staff approved the "Concept of Operations for Tactical Communications Control Facilities (TCCF) in the Management and Control of Tactical Communications." Starting at the same time, the communications equipment that will form the digital tactical communications systems of the future was being developed under the Joint Tactical Communications (TRI-TAC) Program. This equipment includes digital secure telephone terminals, remote unattended digital multiplexers, transmission assemblages, automatic circuit and message switches, and technical control and management facilities with automated assistance. Each of these items of equipment was specified to perform in accordance with the TCCF concept. The TRI-TAC office is currently preparing a performance specification for the AN/TYQ-16 which is to provide automated assistance to the system control element. As part of this effort it became necessary to examine network control structures from a theoretical point of view.

This paper discusses tactical digital communications systems in terms of a common control structure using the principles of systems with distributed control. Tactical communications systems are discussed in terms of their three independent but interrelated networks: the circuit switch network, the message switch network,

and the transmission network. A common control structure is derived for each network taking into account the capabilities of the equipment comprising the network, the TCCF concept of operations, and the basic principles for networks with distributed control. The common control structure is also used to describe the relationship between elements in different networks. These network control structures are then used to describe the required capabilities for the AN/TYQ-16 in support of the system control element. The advantages of the common control structure and the properties of a system using distributed control are also discussed in terms of the required basic characteristics.

INTRODUCTION

Tactical communications systems have always been designed to be survivable, flexible, and reliable and to meet the mobility requirements of the users of the system. The equipment used to realize these systems is evolving from manual to automated. The capabilities of the new equipment and the overall objectives for system performance require rethinking of the control structure for the system.

With the advent of mini- and microprocessors, a great deal of study has been made of systems composed of large numbers of processor equipped facilities. An effective method of control for such systems has been described as distributed control.(1) In order to understand the applicability of a system of distributed control in a tactical communications system the background of control concepts for tactical communications systems are discussed, the basic control structure for distributed control systems are reviewed, a common control structure for the networks in a tactical communications system is derived, and the capabilities required in the system control element of the control structure are elaborated. The advantages of such a control structure in achieving the overall goals of the tactical communications systems are also discussed.

BACKGROUND

In 1973, the Joint Chiefs of Staff approved the "Concept of Operations of Tactical Communications Control Facilities (TCCF) in the Management and Control of Tactical Communications."(2) This concept recognizes that there are four functional levels of management and control in tactical communications systems, the Communications System Planning Element (CSPE), the Communications System Control Element (CSCE), the Communications Nodal Control Element (CNCE), and the Communications Equipment Support Element (CESE). As functional elements, each level of the TCCF represents a combinations of men and equipment that together perform the sub-functions of the overall functions of that level.

The CSPE is responsible for broad system planning and system engineering in terms of system configuration, validation of subscriber communications requirements and detailed transmission network engineering. The time frame which the CSPE normally considers is the next one to five days.

The CSCE, or system controller, is responsible for detailed engineering in response to CSPE direction and dynamic management and control of the system. The CSCE's primary task is to ensure that the system performance objectives established by the CSPE are continuously met. CSCE directed activities normally encompass the ensuing 24 hours.

The CNCE, or node manager, is reponsible for management of all communications network resources within its assigned area of responsibility. The CNCE is responsible for ensuring the availability of the equipment and personnel necessary to establish the operating elements of its network and supervising the operability of this equipment.

The CESE is a component of each operating element, that is, each communications equipment assemblage or deployable item. Its prime purpose is to continuously monitor the operability and performance of its operating element, to detect deviations from directed performance and to report these deviations to operating personnel and/or the next higher control element.

At the same time that the TCCF concept was approved, 1973, the equipment to be used to establish the tactical communications systems of the future was being developed as part of the Joint Tactical Communications (TRI-TAC) Program. This equipment included a secure telephone terminal, a remote digital multiplexer, a radio/multiplex shelter assemblage, automatic circuit and message switches, and a technical control/management facility with automated assistance.

Each item of this equipment was developed with its own CESE capability. The secure telephone terminal can monitor its own operability and, when activated by a user or when interrogated by a circuit switch, give its current operability status. The remote multiplexer also continuously monitors its own operability and, when a failure is detected, can notify a distant monitoring point as well as give a local alarm. The radio/multiplex shelter assemblage contains many components, each of which monitors its own status. The CESE of the assemblage accepts failure indiciations from the components and signifies, both locally and remotely, any change in component operability. The assemblage CESE also monitors the performance of the radio equipment and reports changes as they occur. The circuit and message switches, the AN/TTC-39 and AN/TYC-39, respectively, are stored program controlled switches. The processor in each switch continuously monitors the status of the equipment in the switch and reports changes. The switches also prepare performance reports as part of call or message processing and prepare periodic traffic load and status reports. As discussed above, the switches also monitor the status of the terminals connected to them and report changes in status of the terminals. The technical control/management facility is the AN/TSQ-111. The processor in the AN/TSQ-111 monitors the equipment contained in the AN/TSQ-111, accepts reports from the radio/multiplex assemblages and switches, and monitors the remote multiplexers. The AN/TSQ-111 analyzes the reports which it receives and reports primary failures to its higher TCCF element.

The TRI-TAC Office is currently preparing the performance specification for the AN/TYQ-16, Communications System Control Center, which is to provide automated information storage, retrieval, processing and communications support to the CSCE. In the process of preparing this specification, a careful review was made of the responsibilities of each level of TCCF and the information flow that would be required to support the execution of those responsibilities. This review resulted in the derivation of a common hierarchical control structure for each of the three networks in a tactical communications system. This common structure was also used in resolving the interaction of elements at the same level of control in different networks in response to activities affecting both networks. This common control structure was based on the structural principles of systems using distributed control.

SYSTEMS USING DISTRIBUTED CONTROL

A system which uses the concepts of distributed control normally consists of a large number of operating elements, each with an integral intelligent control element. The operating elements interact with each other and the outside world in accomplishing the performance objectives of the system of which they are a a part. Distributed control systems superimpose on the operating elements a multi-level, hierarchical network of adjustable closed loop control elements. A diagram representing such a control system is shown in Figure 1. Each first level control element, that is, the one which is a component of the operating element is given a set of performance objectives and monitors its operating element to ensure that it meets those objectives. The operating element may encounter disturbance inputs. If the disturbance inputs drive the operating element beyond its range of control, the associated control element will provide a local indication and report the event to its superior second level control element. Otherwise, the first level control element will adjust the performance parameters of the operating element. The first level control element can also accept changes to its performance objectives from its superior second level control element and adjust the performance objectives of its operating element accordingly.

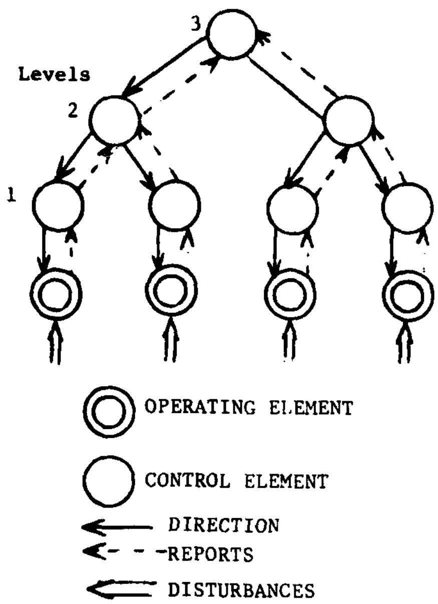


Figure 1. Distributed Control System

The control element at the second level of the hierarchy controls and coordinates the activities of a number of first level control elements. The first level elements may be the same, may each be different but interrelated, or some combination of the two. The second level controller is given a broader scope of performance objectives and translates these objectives into performance objectives for its first level control elements. The second level controller monitors reports from the first level control elements and adjusts performance objectives for these controllers with respect to reported disturbances in order to maximize the accomplishment of its own performance objectives.

The third level controllers similarly control an interrelated set of second level controllers in an adjustable closed loop manner. The performance objectives assigned to the third level controllers are again broader in scope than those of the second level controllers and the diversity of operating elements is greater. The third level controllers break down the assigned performance objectives, assign them to the second level controllers and monitor accomplishment.

TACTICAL COMMUNICATIONS SYSTEMS

Before attempting to discuss the applicability of distributed control systems to tactical communications systems, one must first recognize that a tactical communications system is composed of three separate but interrelated networks; the circuit switch network, the message switch network and the tranmission network. An item of communications equipment can operate in one, two or all three of these networks; that is, simultaneously perform different functions associated with different networks.

The circuit switch network is composed of functional entities called circuit switches, circuit switch loops, circuit switch trunk groups, circuit switch subcribers, message switches, and circuit switch-message switch trunk groups. This last entity interconnects the circuit switch and the message switch networks.

The message switch network is composed of functional entities called message switches, message switch trunks, message switch subscribers, message switch loops, circuit switch-message switch trunk groups, and circuit switches.

The transmission network is composed of functional entities called technical control facilities, transmission groups, transmission links, transmission assemblages, remote multiplexers, circuit switches, message switches, terminal instruments, transmission channels/subchannels, and circuits. The transmission network is interrelated to the other two networks by the use of the circuits provided by the transmission network to realize the loops and trunks of the circuit and message switch networks.

Control of these networks must be in accordance with the TCCF concept. However, the control structure must also take into account the requirement to coordinate the different networks, especially when a change in one of the networks results in a change to one or both of the other networks.

COMMON CONTROL STRUCTURE

Given the characteristics of a system using distributed control, it can be seen that the TCCF concept is compatible with the overall structure. The CESE is equivalent to the first level control element. It

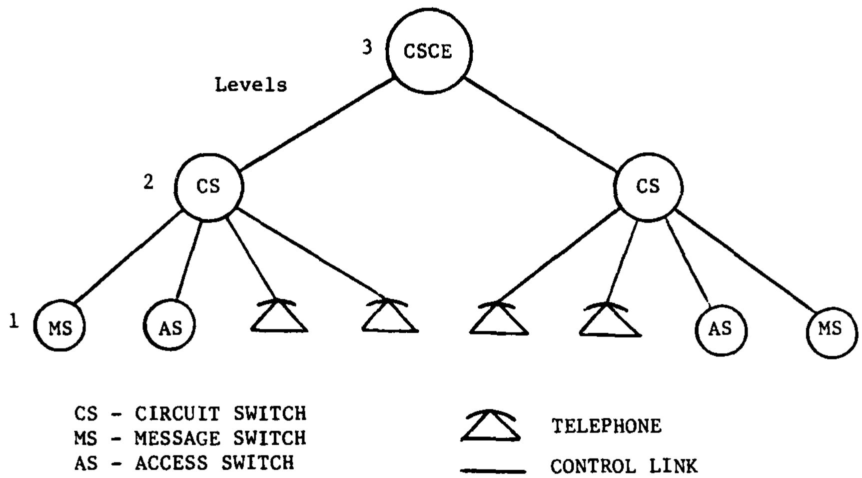


Figure 2. Circuit Switch Network Control Structure

monitors the status of an operating element in accordance with the performance objectives given to it and report exceptions. Similarly, the nodal manager is given broader performance objectives, analyzes them to derive performance objectives for the CESEs which it controls, monitors reports received from the CESEs and takes appropriate action. The CSCE thus controls some number of nodal managers in a similar manner. The CSPE, rather than being a directly controlling element, is the source of direction for the CSCE and views the longer range performance objectives for the system as a whole. Referring again to Figure 1, the TCCF concept can be directly mapped into the distributed control system control structure.

The equipment being developed under the TRI-TAC Program fits well into this common control structure. In the circuit switch network, the telephone terminals have their own CESE that monitors the status of the terminal in accordance with its assigned performance parameters and, when interrogated by the circuit switch, reports on its status. Following the common control structure, this would make the circuit switch the nodal manager of the circuit switch network. The circuit switch does have a CESE to monitor the status of its own equipment, but the processor also monitors more complicated entities, the amount of traffic carried, delays encountered in call processing, and traffic patterns, all of which are in keeping with its role as a circuit switch network nodal manager. The CSCE would monitor the reports from the circuit switches with regard to their traffic functions and provide direction as appropriate. This control structure is shown in Figure 2. It should be noted that in the circuit switch network the message switch and access switches are treated as first level elements since the are treated as a destination for calls just as if they were a terminal. Thus, these elements are shown at level 1.

In the message switch network, the message terminals are at the first level, with their integral CESEs. The message switch is the nodal manager for the message switch network. The CESE of the message switch monitors equipment status but the processor also monitors traffic flow, queues and message delivery status in keeping with its role as nodal manager. The CSCE monitors reports from the message switch with regard to its traffic functions and provides direction as appropriate. This control structure is shown in Figure 3. As shown in the figure, in the message switch network the circuit switch is treated as a level 1 type of equipment since the circuit switch network is used to construct loops to message switch subscribers served by the circuit switch network.

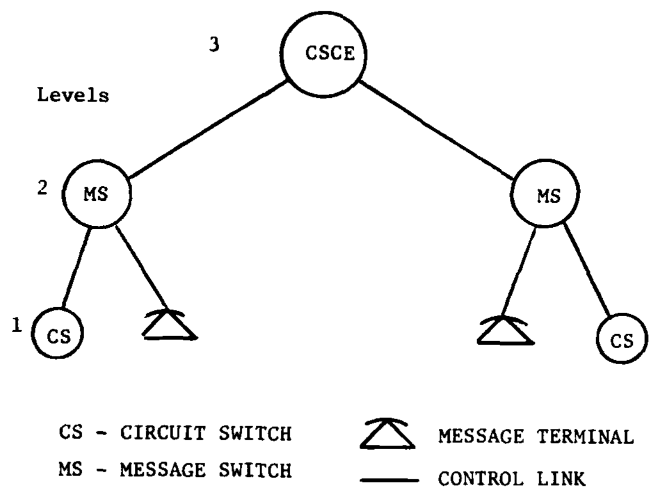


Figure 3. Message Switch Network Control Structure

In the transmission network, Figure 4, the operating elements include the remote multiplexers, the transmission assemblages, and the circuit and message switches. The switches are included since they have integral multiplex equipment. The technical control facility is also included as a first level element since it also has integral multiplex equipment. The management facility of the AN/TSQ-111 is the nodal manager of the transmission network. It monitors the status reports from the first level elements, isolates disturbances, directs corrective action and notifies the CSCE. The CSCE gives specific direction to the management facility of the AN/TSQ-111 in terms of transmission groups, transmission links, channels and circuits. The nodal manager then derives more detailed direction for each of the first level elements and adjusts their performance objectives accordingly.

REQUIRED CAPABILITIES OF THE CSCE

The CSPE sets performance objectives for the three networks of the tactical communications system and establishes their configuration. The CSCE must be able to derive the necessary direction for each nodal manager in each network to implement the network configuration. The CSCE must also monitor accomplishment of this direction. The CSCE must be capable of determining the resources of the transmission network; that is transmission groups, channels and subchannels, that will be used to implement the trunk groups, trunks and loops of the circuit and message switch networks, and of coordinating the interconnection and interoperation of the circuit switch and message switch networks.

The CSCE must also be capable of coordinating the use of resources of all three networks; that is, provide revised performance objectives for the nodal managers, to resolve disturbances which cannot be resolved by nodal managers. Examples of such disturbances would be movement of a subscriber unit circuit switch and message switch subscribers within the network and the failure of a transmission group carrying a circuit switch trunk group, and a message switch trunk.

In the first example, the CSCE would have to determine the impact on the circuit and message switch networks separately and then coordinate the three networks. The CSCE would determine the circuit switch to which the subscriber unit's access circuit switch would be connected and then the message switch to which the unit's message switch subscribers would be connected. The CSCE would then determine which transmission nodal manager would coordinate transmission network access to the subscriber unit and

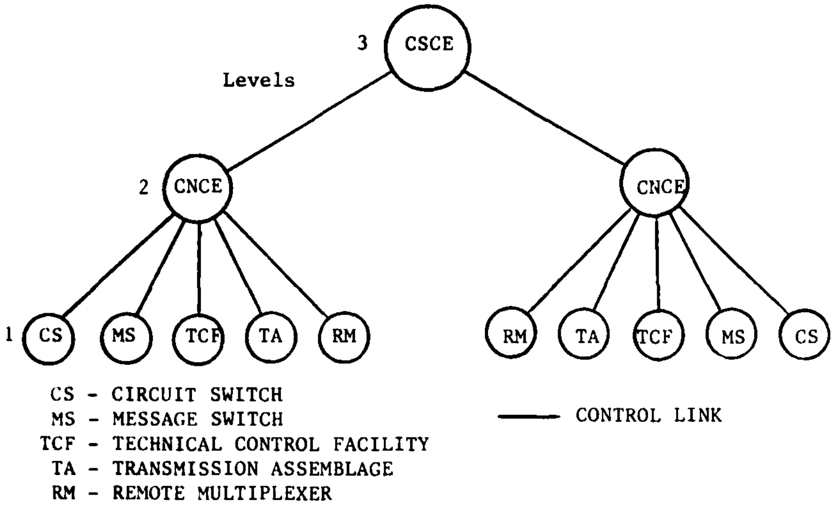


Figure 4. Transmission Network Control Structure

which transmission network resources would be required to implement the connections to the message and circuit switch networks. The CSCE would then direct updating of call and message processing tables of all the circuit and message switches, respectively; for example, the routing tables and fixed directory tables. If one of the message switch subscribers were to be provided access to the message switch network through a circuit switch, the serving message switch would have to be given the subscriber's telephone number. The transmission nodal manager would coordinate the use of transmission resources of the TCF, the circuit switch and message switch to provide the required loop and trunk circuits.

In the second example, the CSCE would have to determine whether transmission resources would be required to reroute the affected circuit and message switch network facilities or whether to adjust the circuit and message switch networks by changing traffic flow; that is, changing routing tables. In either case, or if both types of changes are to be made, the CSCE would have to inform the nodal manager of each network of the required changes and monitor implementation. When the transmission group is restored, the CSCE would have to reconsider its previous decisions to include the ability to cancel direction which had not yet been implemented.

ADVANTAGES OF DISTRIBUTED CONTROL

The concept of a system of distributed control for tactical communications systems provides several advantages in terms of the required characteristics for such systems. First, survivability is improved. Each operating element has an integral monitoring element which immediately informs a more capable element of changes in status. The second level element which receives the report has sufficient information and resources to take effective action to adjust its performance to account for the change in status and to take action to restore any lost capability. The second level elements also have sufficient information to continue effective operations in the event of the loss of the third level element with a minimum degradation of the capability of its network. Reliability is increased by the automatic exchange of status information between levels in a timely manner. Flexibility is increased by having a minimum number of control levels for the exchange of information while, at the same time, having one element resonsible for coordinating the actions of all three networks. The ability to meet the mobility requirements of the subscribers of the system is also improved through effective use of the means to disseminate direction to all affected elements, the shortening of lines of control and single element coordination of the three networks.

CONCLUSION

It has been shown that the TCCF concept and the capabilities of the equipment being developed to implement the digital tactical communications systems of the future are fully compatible with a common control structure for the three networks of a tactical communications system by using the principles of distributed control systems. It was also shown that an item of equipment, for example, the AN/TTC-39 circuit switch, may operate at different levels in each of the three networks thereby complicating the analysis of the capabilities required of the equipment. The overall coordinator of the operation of the three networks, and thus the system, is the CSCE. The capabilities of the CSCE must therefore include not only the capability to control each network individually, but also to determine the impact of activities in any one network on the other two. The advantages of such a common control structure were also discussed.

REFERENCES

1. Kahne, Stephen; Lefkowitz, Irving; and Rose, Charles, Automatic Control by Distributed Intelligence, Scientific American, Volume 240, Number 6, June 1979, pp 78-90.

2. Joint Tactical Communications (TRI-TAC) Office, Performance Specification for the Communications System Control Element (CSCE) of the Tactical Communications Control Facilities (TCCF) (Communications Control Center AN/TYQ-16( )(V)), Specification No. TT-B1-3001-0011, 31 December 1974, Appendix I.

BIOGRAPHY. LTC James A. MacStravic, USA, is the Chief of the Tactical Communications Control Branch, TRI-TAC Office. He has also been Chief, Transmission Branch, Chief, Ancillary Equipment Branch and a member of the Switching Branch in his two tours at the TRI-TAC Office.

LTC MacStravic has extensive experience in communications network planning and control with assignments in Germany and Vietnam. He also prepared the proposal for a nationwide communications system for the Saudi Arabian National Guard.

LTC MacStravic holds a Bachelor's degree in Electrical Engineering from the Massachuesetts Institute of Technology and a Masters Degree in Electrical Engineering from the University of Pennsylvania.

THE NATO III SATELLITE COMMUNICATIONS CONTROL SYSTEM

Mehmet I. Celebiler & Nadir Sanli
NATO Integrated Communications System
Management Agency
Brussels, Belgium
Edward Hirshfield
Ford Aerospace & Communications Corporation
Palo Alto, California

ABSTRACT

This paper describes the NATO III Satellite Communication Control System and the control process. The details of the SATCOM network to be controlled and the elements of control which must be carried out at each level within the SATCOM network and between the SATCOM network and the next higher level of authority are explained to identify the basis for that control. The purpose of SATCOM control is to optimize utilization of the SATCOM network in a timely manner.

The paper is structured to describe the overall NATO Integrated Communication System (NICS) architecture, the NATO III SATCOM system configuration, and the SATCOM control system which is used to implement all command and control functions which pertain. The following paragraphs address the elements described.

NATO INTEGRATED COMMUNICATION SYSTEM ARCHITECTURE

The NICS will be composed of the following communication assets:

a. ACE-High. A tropospheric communications system
b. CIP-67. A line of site communication system
c. Telegraph Automated Routing Equipment (TARE). A number of telegraph message switches
d. Interim Voice Switch Network (IVSN). A voice switch network
e. Leased Lines
f. The SATCOM Phase III Network
g. Technical Control Facilities
h. The Control Overlay

The NICS command and control will be supplied by a series of control centers starting with local control operations (LCOs) at the lowest tier, regional operational centers (ROCs), and Central Operations Authority (COA) at the apex of the control pyramid. The relationship of these assets from a control point of view is shown in Figure 1. The systems listed above are currently in the conceptual phase, design phase, production phase, or are

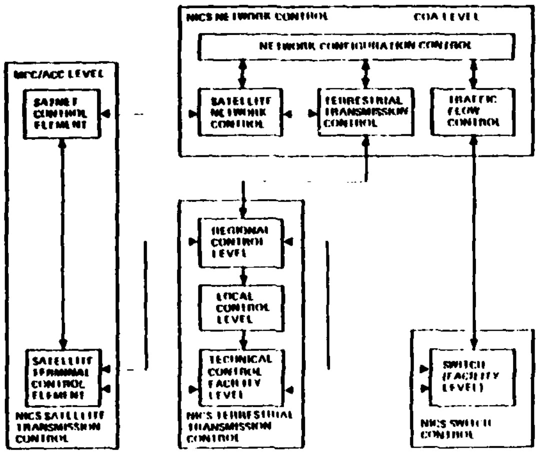


Figure 1. NICS Operational Control

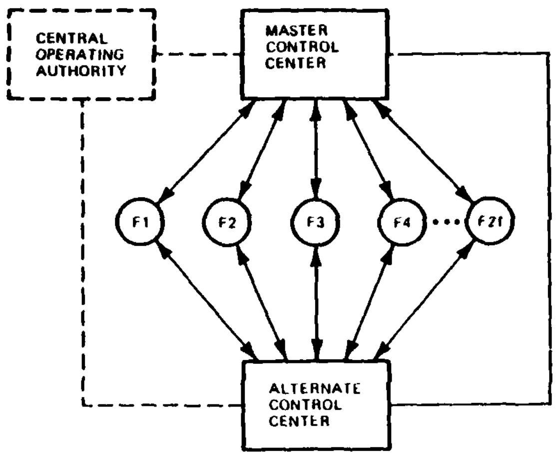


Figure 2. Pictorial Overview of SATCOM Control System

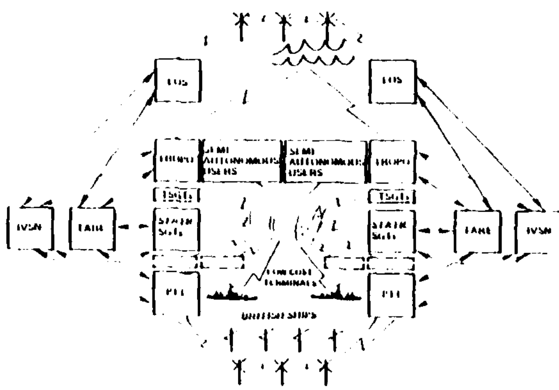


Figure 3. NICS Communication Networks

fully in place. In the 1983 time frame it is expected that these assets will come together to provide a cohesive communication facility for NATO. This paper deals with the command and control aspects of the SATCOM network from the point of view of the internal operations of the SATCOM system and its relationship to the overall NICS.

The SATCOM system provides one of several transmission media available to the NICS. The Phase III SATCOM network is now used to provide dedicated trunk service. As the message and voice switches currently in production come online and the new SATCOM trunks become available, utilization of the SATCOM network will rapidly increase to the point where efficient use of the satellite becomes important. When this occurs in the 1982 through 1985 time frame, a robust command and control capability will become essential. This requirement has been foreseen and the groundwork has been established to provide the required service.

The SATCOM command and control facilities will report directly to the COA. There will be a main and an alternate SATCOM control center, both of which report to COA. All SATCOM terminals report to both SATCOM control centers in parallel. Only the control center in charge issues commands recognized as valid. The two SCCs are each capable of centralized monitoring and control of all NATO SGTs. Figure 2 is a pictorial overview of the two SCCs and SGTs. Each SATCOM terminal contains facilities for automatically monitoring its status, formatting reports, and issuing such reports to the control centers. They also include means for reception of formatted commands from the SATCOM control centers, some of which are automatically executed. The role of the SATCOM Command and Control Network is to:

a. Optimize use of satellite transponder power, and
b. Control and coordinate all other activities required to ensure effective use of the SATCOM terminals themselves.

These assets are intended to provide the variety of services required by NATO. A pictorial view of the relationship between the elements of the NICS is given in Figure 3.

NATO III SATCOM SYSTEM CONFIGURATION

The design phase of the NATO III system has recently been completed and the equipment is now being manufactured. The new system will be completed in mid-1983 and will consist of the system control centers (SCCs), 12 existing static satellite ground terminals (SGTs) modified to SATCOM III standards, 9 new static SGTs, 2 new transportable SGTs, and 2 control centers. The new system will utilize over 200 single-destination QPSK carriers and will provide some 500 voice, 400 low speed telegraph, and 200 medium speed data circuits by the use of time division multiplex (TDM) equipment. The principal characteristics of the modified and new static SGTs will be:

Bandwidth: TX: 200 MHz, RX: 500 MHz

Figure of merit for the receive subsystem (G/T): 35 dB/K

Effective isotropic radiated power: +125 dBW

Carrier to noise density for test tone to quantization noise ratio of 30 dB in a CVSD channel: 41 dB/Hz

SATCOM III Subsystems

A typical static SGT includes the following equipment categories:

a. Power equipment
b. Link equipment
c. Control console
d. System control facilities
e. Beacon receiver
f. Test facilities
g. Test equipment
h. Ancillary equipment

Figure 4 shows the major static SGT components and their functional interconnections in the SATCOM III configuration.

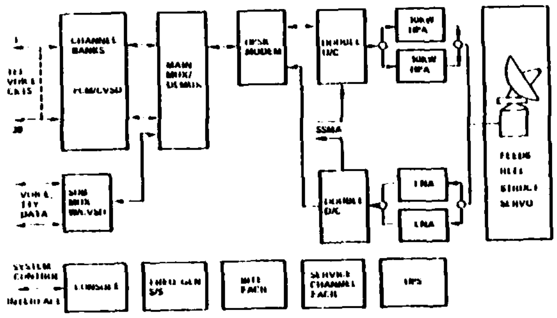


Figure 4. Simplified Block Diagram

These equipment categories are briefly described in the following paragraphs.

Power Equipment

The principal components of the power equipment are:

a. High voltage connection, transformer, and associated primary power supply control and protective services
b. Two diesel-drive alternators with control facilities to serve as a standby power source
c. Static no-break power equipment consisting of batteries, chargers, and inverters with bypass switches, protection, and control equipment
d. Distribution and control boards

Link Equipment

The link equipment extends between the satellite path interface at SHF and the IF interface at 70 and/or 700 MHz. The link equipment is subdivided into primary elements: an antenna and RF system, including a transmitter and a receiver. Each of these subdivisions is briefly explained individually in the following paragraphs.

Antenna System

The antenna system major components include the antenna itself, its mount, a radome, antenna positioning and control equipment, and associated tracking facilities.

The antenna consists of a nominal 40 foot (42 foot for modified SGT, 46 foot for the new) diameter parabolic reflector with a single horn Cassegrain feed and shaped subreflector to provide uniform illumination of the main reflector.

The antenna reflector panels, feed, subreflector, radome structure, and microwave components are designed and manufactured by a special technique to minimize the intermodulation products.

Transmitter

The transmitter is defined as extending from the input of the first or second stage of conversion to the transmit part of the feed diplexer. It includes both first and second upconverters and their associated equipment, followed by dual intermediate and high power amplifiers (HPAs), switching, filtering, and transmission facilities from HPA to the antenna feed. The transmitter is designed for multicarrier operations with a mixture of QPSK and SSMA carriers. It is capable of providing 5 kW CW at the feed. The output of the transmitter can be controlled continuously within the range of 40 dB, locally from the control console at the SGT, or remotely from the SCC.

The conversion equipment employs double conversion technique, with signal combining at 700 MHz.

The first upconverter for the QPSK links translates the 70 MHz output of the associated modulator to any frequency within 700 ± 60 MHz in steps of 1 kHz. The first upconverter for the SSMA link translates the 70 MHz SSMA input to a fixed 700 MHz output. The outputs of the first upconverters are combined by the 700 MHz combiners.

Receiver

The receiver extends from the receiver output port of the feed diplexer to the output of the first or second downconverter. It includes input bandpass filtering, redundant low noise amplifiers (LNAs), and first and second downconverters with their associated signal dividing and distribution networks and transmission facilities.

Low Noise Amplifiers: The redundant LNAs and input bandpass filters, together with the antenna, establish the SGT G/T nominally 35 dB/K over the entire 500 MHz receive bandwidth (7.25 to 7.75 GHz).

Signal Division and Downconversion: The waveguide switch at the output of the redundant LNA/line drivers feeds the online and offline power dividers. The output of the dividers is connected by the input of the downconverters, where frequency translation to the IF occurs. As in the upconverter, the double conversion technique is employed.

Frequency Generation

Duplicated quartz master oscillators with built-in 24 hour batteries are controlled by a dual VLF receiver with built-in chart recorders which allow master oscillators to be compared and adjusted to within 5 parts in 10^{10} against standard VLF transmission.

Baseband Subsystem

General Description

The requirement to implement a digital system and thus completely replace the current analog baseband equipment in the existing SGTs provided an opportunity to design the baseband without restrictions of compatibility with existing equipment. It was thus possible to design this subsystem to meet the requirements of the NICS using new concepts and technology. This in turn provided an efficient utilization of resources. The baseband subsystem was designed to provide the following:

a. Digital communication channels for use as trunks in a switched network
b. A capability to modify the trunk size according to traffic requirements
c. An engineering service network with automatic switching and connections to the terrestrial network
d. Facilities for centralized control of the system

The broad design goals listed above could have been met by a variety of systems. The system designed was therefore further refined to satisfy various technical and operational requirements. Effort was also spent to keep cost, implementation time, and equipment complexity as low as possible. The system which resulted from these considerations has the following characteristics:

Mode of access to the transponder: Frequency division multiple access (FDMA)

Type of Modulation: Quaternary phase shift keying (QPSK)

Type of Multiplexing: TDM

Type of Analog-to-Digital and Digital-to-Analog (A/D-D/A) Conversion: Continuously variable slope delta (CVSD) (32 kW/s) and PCM (64 kW/s); single voice channel per codec

Engineering Service Channels: CVSD, either through a submultiplexer or as single channel per carrier

Control Facilities: Control monitor and display (CM&D) consoles located at each SGT and connected to control centers

These characteristics, together with the design goal *b* above, led to the equipment specifications. Some important features of the equipment are given below.

a. Block Diagram of the Baseband Subsystem

A simplified block diagram of the baseband subsystem is shown in Figure 5. The A/D-D/A converters are in the form of single codec per channel and are placed in a container separate from the multiplexers. This container can accommodate both CVSD and PCM codecs placed on single cards. The submultiplexer (sub-TDM) is used for multiplexing the engineering service channels, medium and low rate data, and telegraph channels. The TDM is a synchronous multiplexer whose data rate is dependent on the number and type of codecs used over the link. The modem uses offset QPSK and contains a two-rate Viterbi convolutional encoder/decoder unit. A service channel associated with the modem is for use in link alignments. It is an analog voice channel transmitted using frequency modulation (FM). The modem is multirate. It can operate at any rate within the limits of 100 kb/s to 10 mb/s.

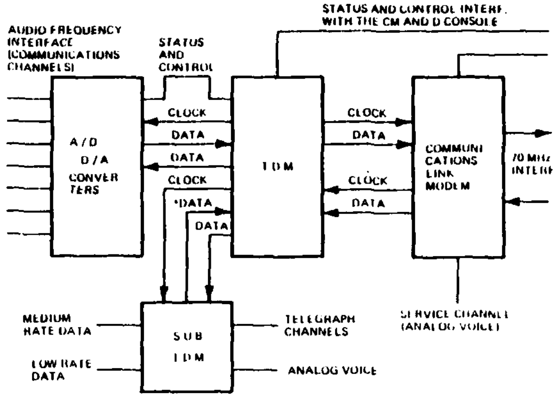


Figure 5. Baseband Subsystem

b. The Sub-TDM

The codecs discussed above provide trunks for telephone traffic, but there is also a need for interstation communication channels for housekeeping purposes. The service channel provides such a facility. This channel does not have to meet the requirements of trunk channels. The use of one of the traffic channels would result in a waste of capacity. On the other hand, the use of a signal processor totally different from the traffic would increase the complexity and consequently the cost of the TDM. The solution to this problem is to use a sub-TDM which has a multiplexed output format identical to the 32 kb/s CVSD codecs. With this solution, the sub-TDM can be built to multiplex digitized speech, data, and telegraph signals which are required for housekeeping and other purposes.

c. The TDM

The role of the TDM equipment is to multiplex a number of 32 kb/s and 64 kb/s synchronous signals. Furthermore, there is a requirement to modify the output rate of the multiplexer according to the number and rate of ports in use. The TDM accepts either 32 kb/s or 64 kb/s synchronous inputs. The TDM must also perform PCM word synchronization. This is accomplished by requiring the TDM to have an aggregate bit rate no more than the sum of the rates at its ports plus an overhead.

Control Monitor and Display Subsystem

The automated CM&D subsystem is based on a dual microcomputer and its associated peripheral equipment. The CM&D subsystem monitors and displays numerous parameters of the SGT and provides commands to the several variable components of the SGT equipment in order to achieve an optimum and efficient operation of the SGTs. Command and control of the SGT equipment may be achieved locally from the CM&D subsystem, or from the system control center(s). The CM&D subsystem monitors and displays:

- Antenna movement and the position (elevation and azimuth angles)
- Ephemeris data for the previous 24 hours
- Performance of the receiver (gain, noise temperature)
- Path loss variations (the beacon signal strength)
- Beacon information (identification)
- Performance of each received carrier (E_m/N_o)
- Power level of each transmitted carrier
- Total power level of the transmitter

Furthermore the CM&D subsystem displays, in color graphic form, the status of the following SGT equipment:

- Antenna position control and drive
- Antenna mode of operation (autotrack, spatial scan, standby, etc)
- Transmitter (upconverters, driver amplifiers, high power amplifiers)
- Receiver (low noise amplifiers, downconverters)
- Beacon receiver
- Local oscillators
- Modems
- Multiplexers
- Link equipment configuration
- Mains power supply equipment
- Ancillary equipment

The equipment makes extensive use of microprocessors and firmware to store, manipulate, and pass information. The CM&D subsystem controls:

a. The Antenna

- By reading its position and driving it to a new position. This is achieved by simply peaking on either the beacon signal or a carrier (step track). This is simply achieved by examining the signal level as a function of antenna position. The algorithm is designed to seek the peak of the antenna main beam by a series of iterative steps, measure, and move on both the elevation and azimuth axes. The aim of the system is to maintain the received signal level within ±0.1 dB of the available maximum signal.
- By driving it to a predetermined position (preset).
- To scan a spatial position in the space with a given pattern in order to acquire a satellite where its accurate position is not clearly known (spatial scan).
- To bring it to a halt (standby).

b. The Transmitter

- By switching between the redundant units.
- By maintaining the output power to a set value.
- By adjusting the output power to a demanded value (this may be achieved by controlling the output level of the driver amplifier (traveling wave tube amplifier) either from the local CM&D equipment or by a command received from the SCC.

c. The Carrier Level Control (CLC) Attenuators

- Control of individual carrier power achieved by controlling the pin diode attenuators inserted in the uplinks. Commands to the CLC attenuators may be given either from the local CM&D equipment or from the SCC through the CM&D.

d. The Number of Channels per Carrier

- This is accomplished by control of modem rate and addition or deletion of channels from the TDM.

The CM&D subsystem accomplishes the above tasks by using:

- A dual minicomputer
- A multiprogrammer and numerous extenders to permit multiplexing of the digital and analog control and numerous signals to the digital format required by the computer
- Dual color cathode ray tube (CRT) display units and associated keyboards for visual displays of the various data and status information and for inputting equipment assignments, performance limits, etc
- Maintenance terminal units (maintenance terminal consists of CRT, cassette tape transport, and associated keyboard) for inputting programs and terminal equipment data, etc

The CM&D system is a focal point of an SGT for the SCC.

All data and status information mentioned above are collected at the CM&D, put into the message format, then transmitted to the SCC. Similarly, the command messages received from the SCC are sorted at the CM&D and directed to the relevant equipment for execution.

Beacon Receiver

The beacon receiver is composed of the following sub units: tracking receiver, beacon measurement unit, and telemetry demodulator. It provides:

a. Acquisition and identification of satellite beacon signals
b. Signal to the antenna drive and control system to accomplish step track
c. Measurement of received beacon carrier power level
d. Measurement of receive gain
e. Measurement of system noise temperature
f. Extraction of SATCOM III telemetry data stream
g. Synchronization with SATCOM III timing sequence

Items *a* and *b* are basically for tracking purposes; items *c*, *d*, *e*, and *f* are for system transmit power control purposes. Item *g* is for SSMA operation.

THE SATCOM CONTROL SYSTEM

Purpose of the Control System

Since the advent of satellite communications services in the mid-1960s, utilizing the full communications capability of the satellite has been a significant problem. The satellite in orbit represents a fixed channel capacity, in terms of power and bandwidth, for carrying military or commercial revenue traffic. Consequently, the problem is to maximize user traffic that is transmitted through the in-orbit capacity. The system control is designed to deal with changing traffic and transponder loading due to the change in requirements and/or transmission properties. The network for which the control system is intended is a configuration consisting of many TDM/QPSK/FDMA single destination carriers whose characteristics may be changed by remote or local electronic control. The system parameters which may be changed by the control subsystem are:

a. Total transmit power for SATCOM terminal
b. Transmit power per carrier
c. Number of channels per carrier
d. Bit rate per carrier

Description of the Control System

In order to properly control these parameters, a number of system characteristics are measured and correlated. These characteristics are:

a. Received signal quality per carrier (BER)
b. Receiver noise temperature
c. Signal bandwidth
d. Signal frequency
e. Satellite total transponder transmit power
f. Received satellite beacon power at each ground terminal
g. Beacon identification code
h. Beacon telemetry
i. Ground terminal equipment status as follows:
1. Type, status, and location of voice channel codecs and data multiplexers per carrier available for use
2. Voice channel codecs and data multiplexers per carrier employed
3. FEC rate employed per carrier and whether or not FEC engaged
4. Equipment fault status and availability of redundant equipment

The quantity and variety of parameters to be monitored and controlled is such that a computer-based control center is mandated. The control system is designed to collect information automatically and periodically from each of the SATCOM terminals, to compare this information to that in a data base maintained in the computer, and to generate appropriate commands to control the parameters listed above. The system is automated to the extent practical. This means that a mix of control center operator intervention and automated processes is employed.

Control System Processes

a. Power Control

In power control, consideration is given to the measured quality of each link, the received beacon level at each SGT, and the loading of the satellite transponder. The receiving SGT measures the quality of the received signal and transmits the value to the master control center (MCC). The MCC compares this measured link quality to a predetermined range. If the measured value is outside this range, a power change command is formulated for the corresponding transmitting SGT. Before the power change command is transmitted, the MCC ensures that the link quality degradation is not due to catastrophic failure of equipment and that the satellite transponder has sufficient power reserve for the change. These are determined from the equipment status, the received beacon level reported by the SGTs and the telemetry transmitted from the satellite. This process, when performed as infrequently as once every 10 seconds, will allow the reduction of the nominal link margin to less than 3 dB.

b. Traffic Control

For traffic control, a number of traffic configurations is stored at each SGT. In each traffic configuration, the capacity of each carrier is specified. The MCC can issue commands to the SGTs to switch to any prestored configuration at a specified time, at which time all the SGTs switch to the new configuration. A special power control algorithm is used during the switchover to prevent modems from losing lock. This control allows reconfiguration of the network to accommodate traffic pattern changes, such as traffic demand variations as functions of time in the day as a result of time zone differential, or to accommodate changes in communications environment.

Control System Hardware

Centralized monitoring and control of the SATCOM SGT network is performed by a minicomputer-based SCC and by a minicomputer-based CM&D subsystem at each SGT.

The SCC receives status information from all the connected SATCOM terminals, processes it into a control computer which informs the control center operator of network status, and generates commands which are disseminated to the SATCOM terminals.

The CM&D subsystem at each SATCOM terminal monitors system status at several hundred hardware points and formats the acquired information to display to the console operator on a CRT display. Further, each CM&D subsystem serves as an interface between the SATCOM terminal and the SCC. It receives all commands from the SCC and decimates them to the appropriate element of the SATCOM terminal. In addition, the CM&D formats all status information and passes it to the control center.

Implementation of the Control Subsystem

The SCC consists of two geographically separated identical control centers which receive all status and performance data from every transmitting SGT in the network. Each control center is capable at all times of performing monitoring and control functions for all SGTs in the network. SCCs communicate with SGTs over satellite links, and with each other over either satellite or terrestrial communication links. During normal operation, one SCC operates in an active (command) mode while the other

operates in a standby mode. Since all SCCs receive identical status and performance data from every SGT in the network, the dynamic status and performance data bases at each SCC are identical and, within the limits of communications delays, are synchronized.

The standby SCC, through the inter-SCC link, can function as a backup link between the active SCC and a SGT when the direct (satellite) link between the active SCC and the SGT has failed.

Each SCC receives equipment status and link performance data from every SGT in the network at the rate of one frame every 2 seconds. Similarly, each SCC transmits power control and link configuration data to every SGT in the network at one frame every 2 seconds. Both incoming and outgoing frames are transmitted by their source twice (rate of one frame per 4 seconds). Upon arrival, each pair of frames is compared in order to detect transmission errors.

SCC link control algorithms use data originating at transmit SGTs, at the satellite, or at the SCC itself, depending on the parameters being computed and on data availability. Each SCC is equipped with an automatic spectrum analyzer (ASPAN) in order to monitor the satellite-transmitted downlink spectrum. Telemetry data from the satellite is monitored at the SCC to determine actual transponder utilization aboard the satellite. Uplink power levels, E_m/N_o, and received beacon power levels monitored at each transmit SGT are reported to the SCC.

Each SCC generates commands to control the total transmit power at each SGT, based on reported and calculated parameters which include operating noise temperature (ONT), carrier power-to-thermal noise density ratio (C/kT), and the energy per bit-to-thermal noise density ratio (E_m/N_o). ONT calculation is based on measured data from ASPAN, as is C/kT. Transponder utilization is based on telemetry data from the satellite or (if telemetry data is not available) on uplink transmitted carrier powers reported from the SGTs.

The SCC controls the configuration of time division multiplexers (MUXs) and QPSK modems at each SGT by downloading configuration data over the satellite link. A network planning function of the SCC allows the network controller to analyze the satellite transponder power required to support a new configuration prior to initiating a traffic configuration change. The algorithm used for new configuration transponder utilization is similar to that used for power control, but is not influenced by actual SGT hardware or satellite transponder limitations. These limitations are displayed to the operator for comparison purposes.

Centralized network control is performed automatically by the SCC, with network planning, data base management, and status or performance reporting being carried out by the operator through an interactive man-machine interface (MMI). The SCC operator console is a color terminal with graphics capabilities. The distributed computer interfaces will support long-term data collection and trend analysis capabilities.

Centralized control of carrier power optimizes availability of satellite power, while distributed SCCs operating in an active (hot) standby mode of operation produce high reliability, availability, and flexibility for the network control function.

Figure 6 shows basic hardware configuration of the control center and its interface with the hosting SGT.

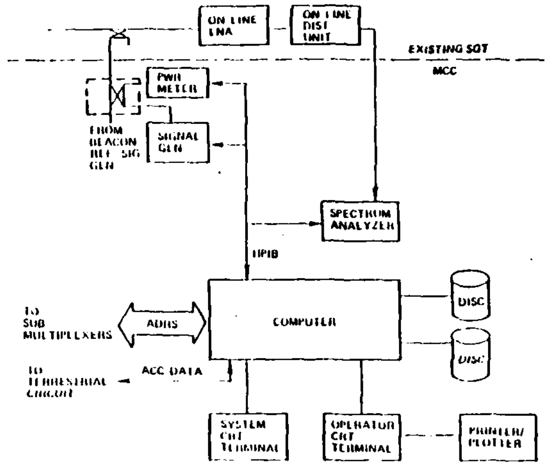


Figure 6. MCC Simplified Diagram

Major components of the system are listed below:

a. SCC processor (Minicomputer HP-2113E)
b. Main memory — 512K bytes
c. Mass storage — redundant 19.6M bytes disk
d. Operator terminal consisting of a color CRT and keyboard
e. Printer/plotter
f. Automatic spectrum analyzer
g. Signal generator
h. Power meter
i. Automatic data reporting system (ADRS) concentrator
j. Control processor
k. Relevant interfaces for the units above
l. Teletype (TTY) concentrators and TTY machines

Two front end processors (ADRS and control) in the system provide a high degree of flexibility in the design of the total system. The processors are used to offload the mainframe CPU.

The control center and the ground terminals communicate through the ADRS (a group of communication channels via the satellite). The number of ground terminals and the number of end users become limiting factors in the design of the total system if they interface directly with the minicomputers inside the control center and the ground terminal. Two microprocessor-based front end processors, the ADRS concentrator and the control processor, are designed to share the workload of the minicomputers and provide greater flexibility in the total system design.

The ADRS concentrator works as a pipeline processor. It receives commands from the control center and distributes them to the ground terminals. Conversely, all the statuses and responses from the ground terminals are funneled through the concentrator to the control center. The control processor resides inside the ground terminals, relays the ADRS data flow, and

monitors the status of the baseband equipments (TDMs and modems). Upon receiving command from the ground terminal, the control processor informs the baseband equipments to switch in/out end user circuits.

The telegraph concentrator provides telegraph message routing from one telegraph operator to another telegraph operator at the SGTs and the network control centers or other selected sites.

SUMMARY

The foregoing describes the NICS architecture and the NATO SATCOM system, with emphsis on the control portion of the SATCOM system. It is believed that the sum total of the SATCOM system and its control elements will compose the most advanced satellite communication network yet fielded. The system is an example of what can be achieved when all of the requirements for such a system are considered as a whole and the development is treated homogeneously. Most other SATCOM networks, both military and commercial, have evolved incrementally. SATCOM control in other examples has been treated as an overlay. In the case OF NATO, the elements required for control were built into the SATCOM terminal equipment hardware and software from the beginning. For this reason it is felt that the results achieved will allow more flexibility and command and control options than might otherwise have been possible. This should allow more reliable and responsive performance than has previously been achieved.

BIOGRAPHY

Edward Hirshfield

Mr. Edward Hirshfield is currently the System Engineering Manager for the NICS SATCOM III Program at Ford Aerospace & Communications Corporation. He has been responsible for the overall system design and implementation since the proposal phase beginning in 1975 and through the contract from 1978 to the present time.

In the past, Mr. Hirshfield has been responsible for receiving systems and receiver designs. He has been at Ford Aerospace & Communications Corporation since 1975. Prior to that he was at the EDL Division of GTE Sylvania for 13 years.

Mr. Hirshfield was granted a degree in Physics at Kenyon College in 1960. He performed graduate studies at the University of Santa Clara and George Washington University. He has participated in numerous seminars and specialized training courses. He holds several patents in receiver technology.

Nadir Sanli

Born in Izmir, Turkey, received his MSEE degree from the Technical University of Istanbul in 1958. He worked for 1 year at the Technical University of Istanbul as a supervisor for telecommunications and acoustic laboratories. He obtained a scholarship from Philips International Institute in 1960, where he made advanced studies in semiconductors and designed several circuits for transistorized televisions.

He returned to Turkey and joined the Standard Electronic Telecommunications in 1962, where he worked as the Test Director for the Troposcatter System built for NATO. He joined the NATO staff in Izmir in 1964 as the Chief System Controller of the Troposcatter System for South East region. He transferred to SHAPE in 1967 as a Project Engineer for the NATO Satellite Communications System, where he was responsible for RF and modulation equipment. Presently working in NICSMA as a senior satellite communications engineer responsible for preparation of the specification, implementation, and acceptance of antenna system, frequency generating equipment, control, monitor and display system, system control hardware, and their interfaces with SGT equipment and other NATO facilities.

Mehmet I. Celebiler

Born in Ankara, Turkey, received his MSEE degree from the Technical University of Istanbul in 1963 and his PhD degree from the University of Pennsylvania in 1968.

He worked in the COMSAT Laboratories, the Scientific and Technical Research Council of Turkey, and the SHAPE Technical Centre. He is presently the Special Technical Advisor to the Chief of Implementation Division in the NATO Integrated Communications System Management Agency in Brussels, Belgium.

Mehmet I. Celebiler

Edward Hirshfield

Nadir Sanli

NETWORK CONTROL IN THE NATO INTEGRATED COMMUNICATIONS SYSTEM — STAGE 1

Paul A. Baiter, D.M.A.
NICSMA
Brussels, Belgium
Wing Commander Keith J. McPhee
U.K. Royal Air Force
Brussels, Belgium
David H. Toy
The MITRE Corporation
Brussels, Belgium

ABSTRACT: In 1970, the NATO Defense Ministers approved a program to develop a common user communications system called the NATO Integrated Communications System (NICS). The aim of the NICS is to provide communications between eligible military and civil authorities of NATO during peacetime, as well as potential periods of stress or conflict. Due to the magnitude and cost of implementing the NICS concept, its development has been divided into a two-stage program. NICS Stage I (1975-1985) includes the procurement and implementation of separate voice and telegraph switching networks along with improvements and additions to NATO owned transmission subsystems. NICS Stage II (post-1985) comprises the progressive expansion and integration of the major subsystems, including the eventual conversion to all-digital operation.

The purpose of this paper is to present an introduction to the NICS Stage I Network Control System (NNCS) whose basic aim is to overlay a control system on the widely different subsystems which comprise the NICS Stage I. Therefore, a brief description of the subsystems comprising the NICS Stage I will be provided, including their built-in control features. This is followed by a description of the planned control organization. Finally, the plans for the evolutionary development of the NNCS and its key features will be described. The NNCS for NICS Stage I is being planned around an analog system so that many similarities with existing communication control systems will be evident, for instance, the Defense Communication System of the United States. The NNCS will be modified as digital facilities are implemented as part of the Stage II expansion of the NICS, but these changes are beyond the scope of this paper.

1.0 INTRODUCTION

In 1970, the NATO Defense Ministers approved a major program to develop a common user strategic communications system called the NATO Integrated Communications System (NICS). At that time, the existing NATO strategic communications were predominantly provided through special purpose dedicated and manual networks configured hierarchically, paralleling the political and military command structure of NATO, The transmission links supporting these networks are derived from a mix of leased PTT and NATO owned facilities. The basic intention of the NICS is to replace these special purpose networks with survivable, flexible, secure, reliable and responsive communications capabilities for eligible military and civil authorities of NATO. This network is to be used for exercising command and control during peacetime, as well as during periods of conflict or stress.

In 1971, the NICS Management Agency (NICSMA) was created and assigned the responsibility for the planning, engineering, procuring and implementing the NICS. The basic concept for the NICS envisaged the creation of a survivable network through the implementation of a large number of backbone circuit switches interconnected by transmission links to form a grid network extending throughout the NATO geographic area. This "nodal network" would be the common user network for all voice, message, and data traffic modes. NICSMA recognized that the magnitude and cost of implementing the NICS concept would require a phased implementation, therefore, its development has been divided into a two-stage program. NICS Stage I (1975-1985) includes the procurement and implementation of separate voice and store-and-forward message switching networks along with improvements and additions to NATO owned transmission subsystems. NICS Stage II will provide significant expansion and integration of the major subsystems, with the transition to a digital mode of operation for all future subsystems.

The basic aims of the NICS Network Control System (NNCS) for NICS Stage I are to provide the communications Operating Control Organization (OCO) with the facilities and procedures to exercise and control and restoral actions necessary to maintain user service in periods of peacetime, tension, crisis and war. The concepts for the NNCS are still in the planning stage; however, initial control activities will be heavily dependent upon manual procedures, supported by voice and message communication facilities, as well as ADP equipment to assist in the maintenance and analysis of system information. Maximum advantage will be made of the currently existing reporting and control facilities, and the features which have been incorporated into the design of the Stage I subsystems.

2.0 NICS STAGE I

The NICS Stage I involves the procurement and installation of two major switched networks, the Initial Voice Switched Network (IVSN) and the Telegraphic Automatic Relay Equipment (TARE) network. These networks will automate some of the existing manual systems through the establishment of separate voice and message switched systems interconnecting facilities in all NATO countries. NICS Stage I also includes the provision of interim secure voice equipment and extensive augmentation of NATO transmission capabilities through modification, refurbishment, and additions to existing facilities. The major elements of NICS Stage I are discussed below and include: IVSN, TARE, SATCOM III, CIP-67, ACE HIGH and miscellaneous line-of-sight microwave radio systems.

2.1 IVSN

The IVSN will provide an automatic voice circuit switched network serving users throughout the NATO Alliance. It will comprise 24 operational switches, located at or near major NATO headquarters, interconnected in a meshed (non-hierarchical) configuration, as illustrated in Figure 1. The interswitch connectivity will be provided through the use of circuits derived from both satellite and terrestrial transmission facilities, with any combination of circuit type making up a particular interswitch trunk group. Approximately 30 percent of the 900 to 1,000 interswitch trunks are expected to be provided through the SATCOM III subsystem. Subscribers can be accommodated by two different means, direct connection between an end instrument and the switch (referred to as a Direct NICS Subscriber) or INS. An INS connected subscriber requires operator intervention to be able to obtain the use of certain network features, such as pre-emption and setting-up conferences. When used in conjunction with Standard Interface Equipment (SIE), a user terminal

IA-59,778

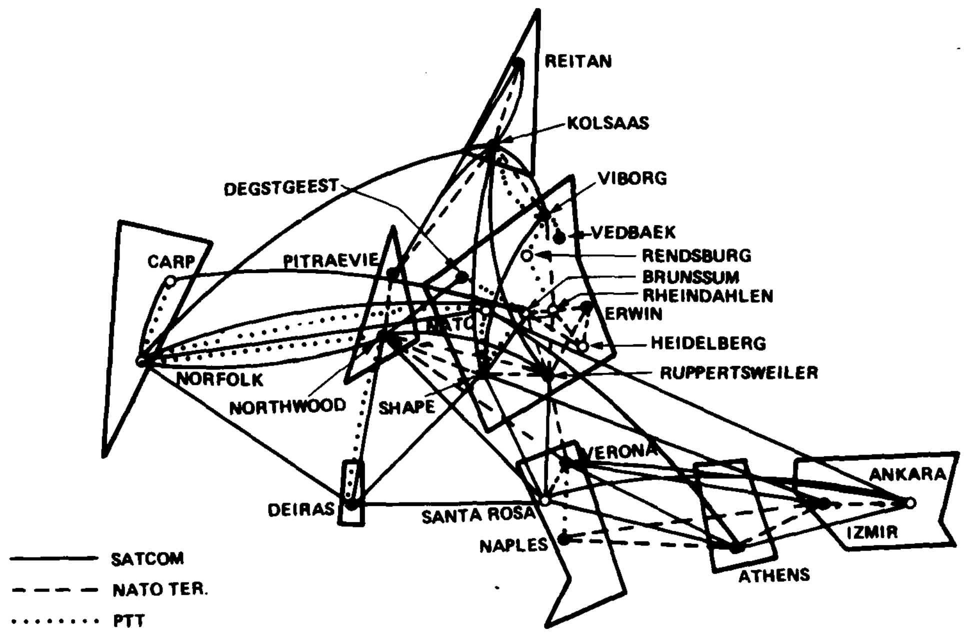


Figure 1. IVSN CONFIGURATION

or P(A)BX can be remotely connected to an IVSN switch through a variety of transmission facilities. The IVSN has been dimensioned to serve approximately 2000 DNS and 7000 INS subscribers with an average busy hour load of approximately 500 erlangs. The switches are stored program controlled, each having a "4-wire" solid state space division switching matrix of up to 1024 terminations which provides local and trunk switching. Interswitch signaling is accomplished via a common channel signaling scheme patterned after the CCITT #6 plan.

The call routing scheme is basically the deterministic spill-forward type, with a capability to fall-back to a previous switch if an all-trunks-busy condition occurs on all routes out of a switch. Up to four possible routes out of a switch to connecting switches can be assigned for each possible destination switch. During call set-up procedures, each switch can identify all the switches already involved in the call attempt and can therefore prevent the occurrence of shuttling and looping. Further, the use of two satellite hops as interswitch trunks in the set-up of any call is prevented, through the utilization of traveling classmarks.

In IVSN, the users are classmarked as having one of five priority levels. If an idle path cannot be found on any of the allowed routing attempts through the IVSN, then the originating switch will invoke a "precedence" search if requested by the calling party. In a "precedence" search, a call of lower precedence can be pre-empted if there are no idle circuits available in the potential routes leaving a switch involved in the call set-up. Pre-emption can also be invoked at the terminating points on a "precedence" call.

The IVSN has another built-in feature, called "query forward," which is intended to reduce the need for external traffic controls by lowering the frequency of ineffective call attempts. The originating switch

directs a "query forward" message to the destination switch over the common channel signaling network. If the called access line is idle or pre-emptable, the originating switch initiates the call routing procedures identified above; otherwise, it returns a busy indication to the calling party. Moreover, a limited set of IVSN user pairs may be given "hot line" service. In this case, the originating switch automatically initiates a FLASH precedence call attempt. The "query forward" feature is not applicable to "hot line" calls; however, pre-emption will be executed on the primary route before searching any alternate route for an idle or pre-emptable circuit.

In addition to automatic alternate routing and pre-emption, there are other control capabilities built into the IVSN switches which can be exercised on demand, either manually or automatically. These controls are summarized in Table I.

TABLE I

IVSN CONTROL FEATURES

CONTROL TYPE	CONTROL ACTION	IVSN CAPABILITY	METHOD OF ACTIVATION
NETWORK ACCESS RESTRICTION	TRUNK RESTRICTION	Certain access lines are denied the capability to make inter-switch calls	Automatic/Manual
	CALL ORIGINATION RESTRICTION	Certain access lines are denied originating service	Automatic/Manual
	CIRCUIT MAKE-BUSY	Specific circuits are removed from service	Manual/Automatic
	CODE CANCELLATION FOR ORIGINATING CALLS	Cancel locally originated calls to specified switch of P(A)BX code(s)	Manual/Automatic
	CODE CANCELLATION FOR ORIGINATING AND TANDEM CALLS	Cancel originating and tandem calls to specified switch or P(A)BX code(s)	Manual
TRAFFIC FLOW CHANGES	ROUTING PLAN CHANGE	Change specific routes for reaching a given destination switch code(s)	Manual
	ALTERNATE ROUTING RESTRICTION	Change the "Routing Protocol" in a given switch (Ranges from Protocol 1, with no routing restriction, to Protocol 5 which allows no alternate routing	Manual/Automatic
	TANDEM LINK RESTRICTION	Change the number of tandem links allowed per call(16)	Manual
	TRUNK GROUP DIRECTIONALIZATION	Specified trunk group not available for outgoing calls (originating or tandem)	Manual

2.2 TARE

The TARE network will be an automatic store-and-forward message switching system consisting of 18 stored program controlled switches. The switches generally will be located at or near major NATO headquarters and will be interconnected with approximately 50 dedicated interswitch trunks, as shown in Figure 2, serving users *via* dedicated low- and medium-speed subscriber circuits. The medium-speed lines and inter-TARE trunk circuits will be encrypted with newly procured equipment while low-speed lines will be encrypted with existing NATO inventory equipments. The TARE design provides for modular sizing of the switches with the maximum capacity being 100 low-speed and 20 medium-speed user terminations and on-line storage capacity for 25,000 messages.

The TARE switches contain built-in routing capabilities to enhance network operation under network damage conditions. The switches have the capability for up to six levels of precedence (four are presently designated). Both deterministic and automatic alternate routing schemes are built into the TARE switches. In the case of deterministic routing the TARE routing tables include a normal route, a reserve route and an alternate route; while in the case of automatic alternate routing, a destination TARE is defined.

In addition to the precedence and flexible routing scheme, there are other control capabilities built into the TARE switches which can be exercised on demand, either manually or automatically. These controls are summarized in Table II.

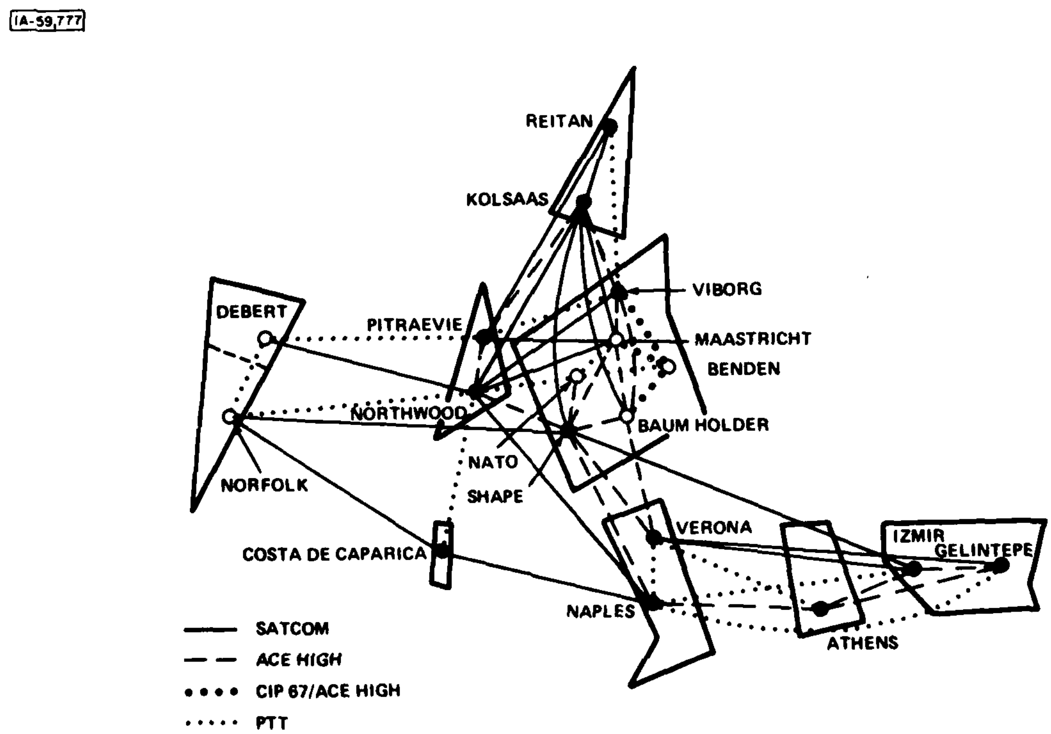


Figure 2. TARE NETWORK CONFIGURATION

TABLE II

TARE Control Features

FUNCTION	CONTROL ACTION	TARE CAPABILITIES
ALTERNATE STATION DELIVERY	- Route Messages to Other Subscriber Facilities for Handling	- Reserve Route Commands - Diversion Commands - Automatic Alternate Routing - System Status Message - Queue State Data - Service Messages
ALTROUTE OF INTERSWITCH TRAFFIC	- Change Normal Route of Messages in Network to Bypass Failed or Congested Trunks and/or Switches	- Automatic Altroute Routing - Close/Open Interswitch Route to Low Precedence or All Traffic - Diversion Commands - Queue State Data - Service Messages
CIRCUIT ALTROUTE (SUBSCRIBER)	- Provide Multihoming of Critical Subscribers to Alternate Switch	- Dual homing of Critical Subscribers
TRAFFIC INTERCEPT CONTROL	- Route Messages to Special Storage, Removing Traffic from In-Transit Store	- On-Line Holding Store - Extended In-Transit Storage - System State Data Retrieval - Automatic Reentry from Holding Store Upon Route Opening - Service Messages
NETWORK INPUT CONTROLS	- Throttle/Inhibit Subscriber or Interswitch Traffic Into Switch - Control Traffic Destined to Certain Areas	- Automatic Line Protocol - Input Channel Closure - MINIMIZE

2.3 Transmission Facilities

The major NATO-owned transmission systems supporting the NICS Stage I will be:

- the ACE HIGH tropospheric scatter and line-of-sight (LOS) system, a radio relay system in the Allied Command Europe area which was installed in 1961;
- the SATCOM III system consisting of redundant space segments and 21 static ground terminals, as well as 2 transportable terminals, which is scheduled for completion in 1983; and
- the CIP-67 LOS microwave transmission network in the central region of Allied Command Europe which is expected to be completed by 1982.

The ACE-HIGH network is the primary terrestrial transmission system of NATO and will provide both dedicated and common user circuits. It consists of a backbone route of 50 over-the-horizon troposcatter links extending from Northern Norway to Eastern Turkey, which has a number of branches but limited alternate routing possibilities. It is supplemented by a number of microwave, cable and PTT facilities to connect the user complexes to the backbone route. ACE-HIGH is an FDM/FM analog transmission system which carries approximately 600 voice and 300 TTY channels. NICSMA is currently undertaking the system planning for the digital replacement of ACE-HIGH and anticipates implementation beginning in 1984, with completion by 1987.

The current control of the ACE-HIGH is handled on a regional basis through Primary Control Centers (PCC's) located at key transmission nodes of the system. These PCC's have limited capabilities for monitoring and directing the ACE-HIGH system performance and operations. The control of

these ACE-HIGH multi-channel transmission facilities is accomplished entirely through manual processes, supported by dedicated voice and TTY orderwires. These ACE-HIGH service channels include an omnibus voice orderwire, an express voice orderwire with dialing capability and an omnibus TTY orderwire. Status change reports are generated manually on teleprinters at the manual radio sites and forwarded via tape relay to the appropriate level of the OCO through the controlling PCC. Control arrangements for ACE-HIGH will remain virtually the same until the conversion to digital operation is implemented. Appropriate expansion of the system control features will be specified as part of the overall replacement project.

The SATCOM III subsystem will provide a significant portion of the circuitry to support the NICS Stage I connectivity. It is being designed to satisfy the requirements for the IVSN, the TARE network, dedicated circuits, itinerant subscribers and mobile users. The SATCOM III program includes an expansion of the existing SATCOM II ground segment from 12 to 21 static ground terminals and the addition of 2 transportable ground terminals. Furthermore, the existing SATCOM II system which operates in the FDM/FM/FDMA mode will be converted to digital operation. The SATCOM III system is being implemented to operate in the digital mode with time division multiplexing of digitally encoded speech signals, forward error correction and QPSK modulation. It will employ frequency division multiple access and single destination carriers, with each carrier being encrypted. The planned configuration will provide in excess of 500 duplex voice channels. Analog-to-digital conversion will occur at the ground terminals at the voice frequency level.

The control facilities being built into the SATCOM III facilities are described in another paper at this symposium so they will not be elaborated upon here. However, the basic objectives of the control subsystems are to allow:

- centralized control of each carrier power;
- central control of circuits through link capacity management;
- centralized monitoring of network status.

The CIP-67 program is an LOS microwave transmission network that is configured to improve and expand services in the central region of Allied Command Europe. It consists of a semi-hardened backbone with a number of unprotected sites and a forward line of transportable radio relay stations. It will contain approximately 60 radio relay stations and utilize conventional FDM/FM analog transmission equipment. The individual links can be equipped to provide a maximum capacity of 300 voice channels. Installation is expected to be completed by 1982.

CIP-67 includes a transmission monitor and control subsystem which will be considered for application to the transmission remote supervisory and control (RSC) concept being planned by NICSMA to support the NNCS and future terrestrial transmission enhancement/expansion programs. The RSC concept applied to CIP-67 includes the provision of two sector control centers (SCC's), with each SCC controlling two sectors of the network, and a regional control center (RCC) which monitors all supervisory and control information passing over the orderwire channels of the radio equipment. The RCC will be able to replace either or both SCC's. Each control center will be provided with a minicomputer for management of the data collection, processing and presentation of the alarm and status conditions from each station. The equipment at each radio site will be uniquely addressable and be connected to all the monitor and control points within the station. Routine status information will be transmitted by each station when polled, but the site equipment will react to certain alarm information on its monitor points by interrupting any existing communication on the reporting line and then immediately sending the alarm information to the SCC and RCC. The status and control information channels will be configured with four loops passing through each SCC. The transmission of information over each loop can be performed in either direction to prevent an outage from isolating other radio relay sites. The equipment at each site (including the control centers) will also transmit information in both directions to be able to interrupt the polling sequence. Independent transmission channels between each sector and the RCC will be established, bypassing the SCC's, to allow the RCC to monitor any sector in the event of the loss of an SCC.

3.0 NICS MANAGEMENT AND CONTROL ORGANIZATION

The responsibility for management, operation and maintenance of the NICS has been assigned to the Controller Central Operating Authority (CCOA), a position reporting to the Supreme Allied Commander of Europe (SACEUR). The CCOA is a collateral assignment for the Assistant Chief of Staff, Communications and Electronics (ACOS CANDE) at SHAPE. However, the CCOA and ACOS CANDE roles are supported by separate staff organizations. The CCOA is supported by a hierarchical Operating Control Organization (OCO). The OCO is headed up by the COA organization located at SHAPE Headquarters, at Casteau, Belgium. Below the COA, operating control is delegated to five Regional Operations Centers (ROC's) based upon the five geographic areas of NATO, and collocated with the headquarters for SACLANT, CINCHAN, AFNORTH, AFCENT and AFSOUTH. The controller of each ROC, as for the CCOA, also serves as the Communications and Electronics Chief of Staff for the collocated Major NATO Command or Subordinate Command. Subordinate to each ROC are a number of Local Control Organizations (LCO's) which have been designated according to geographic areas within each region. The lowest level in the OCO hierarchy are the Operating Units (OU's) which are located at the NICS communications sites and are staffed by technicians in accordance with the complexity of the equipment installed. The SATCOM control is an exception to the hierarchical structure based on geographic distribution. SATCOM control is exercised by the COA through the Master Control Center (MCC) at Kester, Belgium (site of a Satellite Ground Terminal SGT) or the Alternate Control Center (ACC) to be established at Oakhanger, England. The ACE HIGH system control facilities currently include a number of Primary Control Centers (PCC's) which will be absorbed into the OCO. However, the PCC in the central region is expected to exist as a separate facility, at least until the ACE HIGH replacement project is completed in the late 1980's.

In general terms, the COA is responsible for exercising operating control of the NICS, which includes control of the operations, maintenance and logistics support. In order to carry out these functions, the COA will contain an operations element to deal with minute-by-minute activities and a staff element to support those activities which are more long-term in nature, as well as provide technical expertise for the operations branch. The major functions or activities carried out by the COA are:

- develop, maintain and direct implementation of restoral plans;
- maintain overall network and subsystem status;
- direct network configuration changes;
- apprise command elements of the communications status;
- direct deployment of mobile assets;
- coordinate restoral actions with PTT's and national agencies;
- supervise activities of the lower echelons of the OCO.

The controller of each ROC is functionally responsible for the management, operation and maintenance of the NICS facilities within his defined geographic region. In this role, the ROC follows the directives and procedures as developed by the COA, amplifying them as necessary to accommodate local conditions. Due to the diversity in facilities provided to each of the several regions, it is anticipated that the scope of the day-to-day operations will vary among the five ROC's. However, a key requirement is for the ROC's to be able to function independently of the COA if necessary; therefore, many of the COA day-to-day control functions are replicated at the ROC's, although the level of activity will differ in both detail and quantity. In addition, the ROC's will be responsible for:

- arranging for depot maintenance;
- supply activities;
- inspection of facilities;
- manpower provisioning.

The LCO will have responsibility for particular Operating Units, as specified by the COA and parent ROC organization. While the ROC's are basically similar in their responsibilities and functions, the LCO's will vary tremendously in terms of their roles in controlling the NICS. The span of

control of LCO's can vary from, for example, overseeing a few radio relay sites to being responsible for a number of switch sites, as well as a large number of radio relay sites (SATCOM, ACE HIGH and microwave radio sites). The common thread for LCO's will be the management responsibility over the facilities and manpower under its control, while their day-to-day operating control activities will be diversified. LCO's have also been identified as the focal point for user complaints that the local maintenance forces have been unable to resolve. Where appropriate, mobile maintenance teams will be stationed with an LCO.

The Operating Unit (OU) is the lowest echelon in the OCO and operates on a 24-hour-a-day basis. Included in this category are switch sites and manned transmission relay sites (SGT's or terrestrial transmission facilities). As a rule, each Operating Unit will have a supervisor who is responsible to his parent LCO or ROC commander. Operating control over an operating unit, however, may come via a different route as in the case of SGT's. In general, the functions of the Operating Units are to:

- perform fault isolation in conjunction with other Operating Units and/or secondary site personnel;
- perform scheduled and unscheduled maintenance;
- implement service changes;
- implement controls or restoration actions as directed;
- report to higher echelons;
- monitor equipment operation within or connected to the Operating Unit facilities.

4.0 NNCS PLANS FOR NICS STAGE I

The NNCS will provide for visibility of the NICS from all appropriate control levels and provide the means for the Operating Control Organization (OCO) to exercise control over the network. In this regard, the NNCS is planned to obtain and maintain the status and performance of all NICS circuits so that appropriate alternate routing or restoral can be directed for any portion of the NICS. Therefore, the terrestrial transmission circuits, SATCOM circuits, and PTT/Military/National circuits used for NICS are to be covered by the NNCS data base. The NNCS will also provide for centralized visibility and control of the NICS switched systems. Both the IVSN and TARE networks will provide data to the OCO through the NNCS for analysis of traffic flow, switch performance, failures, and other parameters. This data will provide the OCO with the information necessary to control the switched systems. Control directives to the switches will be facilitated by the NNCS on a near real time basis so that the switched network is protected from traffic overloads as well as controlled to account for failures or desired reconfigurations. Thus, the NNCS is planned to encompass the NICS transmission media and switched networks permitting analysis and control from the level where the best network visibility exists.

4.1 NNCS Requirements and Objectives

The NNCS objective is that the system shall be able to generate, transport and process sufficient information to enable the OCO to direct the maintenance of the best possible service under all conditions of system operation, including normal, failure, stress and damage. In this context, service is to be assessed in terms of grade of service, accuracy, speed and security. Thus, the control system's overall performance is measured in terms of its contribution to maintaining the service provided by the NICS under all possible conditions. The minimum acceptable standard is to maintain, at any time, those communications designated as vital by the command elements. The actions concerned relate to network configuration, data management, restoral and reconstitution. In order to support these actions in a real-time environment, it is necessary to provide hardware and software to automate data collection, processing and dissemination for the OCO. There are two general areas to consider in automation: first, is network configuration; second, is status of the network operations. The network configuration can best be defined as the stable condition of the network at a given time. There is, therefore, a requirement to maintain an up-to-date data base on configuration information to include: connectivity, termination equipment, type of service, and operational switches. The status of the network must then be overlayed on the network configuration information to correlate the data and evaluate the impact of any change on network performance. In

order to react to changing conditions in sufficient time, automation of data collection, processing, and display is necessary to provide the means of obtaining the information in real-time, correlating the information, and displaying the information required for the decision process in a timely manner, varying from minutes to hours, depending upon the particular situation.

Closely related to the basic control functions is the long term system management function, which includes performance assessment and the consequent system planning and engineering to accommodate changing conditions and requirements. Because of the close association between the control and management functions, the same information support base will be utilized. However, the long-term management function will require more detailed information than can reasonably be supported by the NNCS in its early configuration and consequently must await the implementation of an automated data collection system. The requirements can be summarized as follows:

a. To enable the OCO to receive, store and correlate automated reports from TARE and IVSN switches, as well as information reports on the transmission systems, on a near real-time basis;

b. To achieve sufficient visibility on a timely basis to effectively exercise day-to-day management and control of the NICS during the transition from implementation to operational status;

c. To provide the basis for development of logical, effective procedures/plans for management and control of the NICS;

d. To provide the necessary ADP facilities to record the network configuration and subsequently overlay the network status, which will provide network assessment on a real-time basis for management/control purposes;

e. To provide the capability for collecting and maintaining current network status information and subsequent correlation of data for decision making in a timely manner;

f. To provide for collection and correlation of traffic information, equipment utilization, and grade of service for long-term performance analyses;

g. To enable controllers to respond to user complaints with definitive data concerning the actual service being provided;

h. To possess as much flexibility as necessary to enable evolutionary development of the NNCS and expansion without major redesign.

4.2 NNCS Implementation Strategy

The NNCS will evolve based upon operational experience and is being planned with flexibility to adapt as experience is gained. A progressive development containing six independent but related steps are being planned. A more detailed description of each of these steps follows:

NNCS STEP 1: The first step will equip all of the OCO control centers with the basic communications facilities required to collect information about the NICS configuration and performance, record that information, and pass instructions to all subordinate control and operating units. Information processing and display will be mainly manual; therefore, the immediate information flow will be limited to the essential minimum necessary to detect major network changes which require control action. More detailed information, which is not time critical, will be collected and analyzed to the extent that the system capacity, in terms of equipment and personnel, will allow. The COA will be provided with remote terminal access to the NICS Network Data Bases and visual display terminals will be installed to assist operators in handling NNCS reports received at the COA, ROC's and LCO's. The primary voice and TTY communications connectivity will eventually be via common user means but initially existing temporary orderwire communications will be used until the TARE and IVSN systems are operational.

NNCS STEP 2: A capability for remote reporting from the IVSN access switches will be provided. The required software modules and interface hardware will be developed to permit rapid handling of normal system status data, urgent status/control informa-

tion, and also routine summaries which are not time sensitive. The data will be extracted and presented to a standard interface point with the format and content required by the control centers. An automatic means of transporting the data will eventually be available; however, data will initially be limited to essential traffic and manually relayed from the TCF.

NNCS STEP 3: The capabilities to automate many of the network control functions will be developed. Report processors will be provided to obtain data from the switched systems and Remote Supervision and Control (RSC) subsystems of transmission facilities. The automated data processing equipment at the COA, ROC's and LCO's will be capable of accepting reports from TARE's and IVSN Switches automatically, and from the transmission subsystems and TCF's either manually or automatically. Reports will be stored and displayed in simplified standard formats and forwarded to other interested control centers as required. ADP applications will be specified to permit fielding the capabilities separately. The functions will be implemented starting with transmission systems, adding switch data, contingency planning and finally performance assessment. Data base management will be developed as an integral part of all the other functions and data display facilities will also be provided using projected graphics onto large screen displays for the COA. The addition of ADP systems in the OCO will improve the response time and will support the concept of decentralized network control by providing the following functions:

a. Transmission Systems Control. A transmission system/circuit data base will be continuously updated with status information concerning stations, radio paths, and groups. This information will be correlated with data on circuit allocations, user identities, and eventually, contingency planning information. The impact of failures or degraded conditions will be evaluated to determine appropriate control actions with rapid response times.

b. Switch Control. Equipment and traffic status reports will automatically be made available to update the control data base. Flags will be provided automatically to identify to the operators that failures or other abnormal conditions have occurred that may require network control actions. Reports will be available for recall by type, switch and network-wide to assist in developing control solutions.

c. Data Management. Mechanisms will be provided to maintain data bases current through a flow of information to all sites where system data bases are resident. Procedures will be established to review and enter new data in order to ensure accuracy.

d. Contingency Planning. ADP support will provide the capability to store pre-determined contingency plans which can be quickly retrieved and implemented. More importantly, contingency solutions for unplanned situations can be developed in real time through rapid assessment of network conditions.

e. Performance Assessment. The capability to assess long term performance will be developed. Network norms and deviation from the norms will be made available through the processing system to permit evaluation of the deviations and facilitate directives to correct abnormal conditions.

NNCS STEP 4: It is expected that the NNCS will require extensive simulation modeling to develop accurate and proven control strategies to be used as a basis for further automation of the control process. This step provides for modeling to determine the enhancements of the NNCS that should logically be added to improve the system.

NNCS STEP 5: This step provides for system enhancements that are identified both from the modeling effort of Step 4 and from lessons learned through control experience with the operational network. It is expected that the majority of NNCS improvements under this step will involve addition or changes to the software.

NNCS STEP 6: The sixth step planned for the NNCS evolution will be to integrate the circuit test and the remote supervision and control functions into the system. This

will be achieved by enabling remote circuit testing from LCO's, using automated test equipment at TCF's. This arrangement coupled with the other control features of the NNCS will enable the OCO to determine the transmission quality and through correlation of information will ensure the best allocation of serviceable resources to meet user requirements.

4.3 NNCS Schedule

Implementation of the six-step NNCS program is expected to begin in mid-1981 with the realization of the full range of perceived NNCS capabilities in the late 1980's. The NNCS program plan is designed to be evolutionary, so that the control capabilities are incrementally improved with the implementation of each step. Further, software enhancements envisaged for Step 3 will be progressive and new software modules implemented in discrete increments.

It should be noted that NICSMA has yet to receive approval for this program through the NATO committees, so that these plans are subject to change in the future.

5.0 CONCLUSIONS

The existing communications capabilities consist of special purpose, dedicated, and predominantly manual networks structured in a hierarchical configuration that reflect the NATO political and military command structure. The transmission links are a mix of leased PTT facilities and NATO-owned facilities. The procedures and capabilities of the control organization supporting this system are, therefore, basically manually oriented. Control for terrestrial and satellite facilities is distributed on both a regional and functional basis.

With the realization of the NICS Stage I and its associated control system the NNCS, the manually oriented capability will be evolved on a gradual basis to a highly sophisticated and automated capability. In order to facilitate the transition and at the same time provide enhanced survivability of the control system, major emphasis has been placed upon providing the NNCS with adequate flexibility to allow easy distribution of control functions and capabilities among the approved levels of organization control.

The challenges associated with effecting this evolution are numerous and are further constrained because of the lack of adequate experience within NATO in the area of switched telecommunication systems control. An additional factor influencing the evolution of the NNCS is the planned transition of the NICS from a predominantly analog system to a switched digital system in the future. This transition will present an ever greater set of challenges to be met in the future enhancement of NNCS.

BIOGRAPHY

Paul A. Baiter

Paul A. Baiter is currently serving as a Network Control Engineer with NICSMA in Brussels, Belgium. Prior to this position, he spent eight years with the Defense Communications Agency both in Reston, Virginia, and in Taiwan, working on diverse communications projects. Earlier experience includes work with laser fuze systems and missile tracking ship systems with the U.S. Air Force.

He holds Bachelors and Masters degrees in electrical engineering with extensive doctoral studies in electrical engineering and also holds a Doctorate of Arts (D.M.A) degree.

Keith McPhee

Wing Commander McPhee has been working in the Systems Planning and Engineering Division at NICSMA since 1978, with prime responsibility for the NICS Network Control System planning. Beforehand, he worked in communications control for the United Kingdom Defense Communication Network and in Communications Operations with the U.K. Far East Air Force.

He has been a registered professional engineer in the U.K. (C.Eng. M.I.E.E.) since 1971.

David H. Toy

Currently, Mr. David Toy is a systems engineer with The MITRE Corporation, serving as a technical advisor to the NATO Integrated Communications System Management Agency in Brussels, Belgium, through the U.S. Defense Communications Field Office. Prior to this assignment, he has worked on a number of different communications projects,

the most recent being a requirements definition study for the U.S. Navy. He previously worked for the Bell Telephone Laboratories, 1965-1972, in the switching systems engineering division at Holmdel, New Jersey.

He received his BSEE with Distinction from the University of New Mexico in 1965 and an MSEE from the University of Pennsylvania in 1966.

AD-A103 830 MITRE CORP BEDFORD MA F/G 17/2

PROCEEDINGS OF THE MILITARY COMMUNICATIONS SYSTEM CONTROL SYMPO--ETC(U)

NOV 80 S HARRIS, J HELLER

UNCLASSIFIED M80-30 NL

2 OF 2

AD A
103830

END
DATE
FILMED
10-81
DTIC

EVOLUTION OF CONTROL IN THE DEFENSE SATELLITE COMMUNICATION SYSTEM

P. Jeffrey Bogert
Stanford Telecommunications Inc.
Sunnyvale, California

ABSTRACT: This paper describes the evolutionary development of the Defense Satellite Communication System (DSCS) Control Segment from the current largely manual system to the deployment of the Real Time Adaptive Control System (RTACS).

INTRODUCTION

The Defense Satellite Communication System (DSCS) provides a flexible, multi-trunk, multipoint, wide-band, long-haul transmission system which interconnects with Defense Communication System (DCS) terrestrial elements via DCS technical control facilities (TCF's) located at each of the DSCS Earth Terminals. DSCS consists of satellite networks composed of satellite communication relay terminals in synchronous orbits and earth terminals for control and communication interconnectivity.

DSCS requirements for technical control of satellite transmission facilities differ significantly from commercial equivalents in that unpredictable changes in traffic requirements must be implemented rapidly and reliably, and minimum connectivity must be maintained under jamming conditions. In addition, DSCS must accommodate a wide variety of terminal sizes, and dynamically changing terminal deployments, as shown in Figure 1.

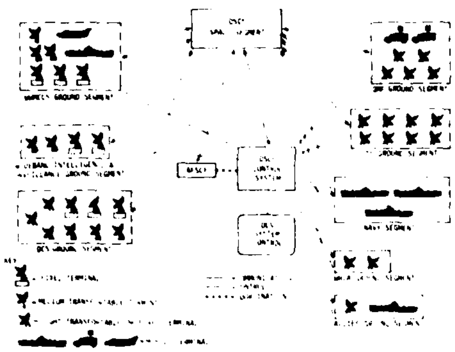


Figure 1. Major DSCS Elements

The DSCS is evolving from a relatively low capacity static system to one with the capability to provide high capacity, flexible communications services in support of the World Wide Military Command and Control System (WWMCCS), the DCS, and special users. As part of this evolution a new space segment has been developed. The DSCS III Space Segment will carry these Multiple Beam Antennas that can be configured to provide varied coverage patterns such that antenna gain is allocated to desired accesses while at the same time rejecting interference sources. As the system grows in capacity, flexibility, and complexity, efficient operation becomes more dependent upon the control segment.

To meet these challenges, the DSCS Control Segment is evolving from a largely manual system to the real-time adaptive control (RTAC) system.[1] The Defense Communication Agency (DCA) has planned a transitional strategy that consists of the following developments:

1. The Pilot Control System (PCS) and PCS Extension.

2. The Satellite Configuration Control Element (SCCE), an X-band TT&C system.

3. The Control Coordination Subsystem (COSS) and AN/USC-28 Spread Spectrum Modulation Equipment (SSME).

4. The DSCS Operational Support System (DOSS) and Resource Allocation Software (RAS).

5. The DSCS Automatic Spectrum Analyzer (DASA).

6. The RTACS.

CONTROL CONCEPT

The DSCS, as a transmission medium for the DCS, is under the operational direction of the Director, Defense Communication Agency.[2] The DCA Operations Control Complex (DOCC) is the control hierarchy through which the Director, DCA exercises control of the DCS and DSCS. The elements of the DOCC primarily concerned with Control of the DSCS are shown in Figure 2. The highest level of control within the DOCC is the DCA Operations Center (DCAOC). There are two Area Communications Operations Centers (ACOCs) and eight DSCS Operations Centers (DSCSOs) located worldwide.

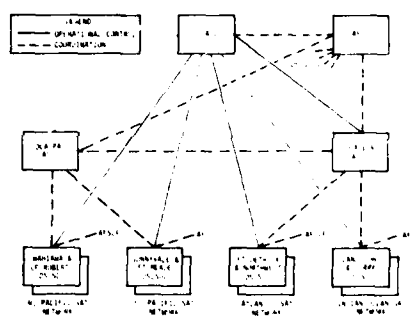


Figure 2. DOCC Elements for DSCS Control

Current Control Concept

At the current time, the DCAOC exercises operational direction over the DSCS through the DCA Area Communications Operations Centers (ACOC's) and the Air Force Satellite Control Facility (AFSCF). The AFSCF supports the DCAOC by accomplishing all telemetry, tracking and command (TT&C) functions for the DSCS II satellites in accordance with DCAOC requests or established procedured. Control and monitoring of satellite orbital and health parameters is exercised by the AFSCF using S-band TT&C. The ACOC's exercise operational direction of the DSCS satellite networks as assigned by the DCAOC. The DSCS Satellite Communications (SATCOM) network controller, an element of the ACOC, is responsible for the control and management of all earth terminal

accesses to the satellite.

RTACS Control Concept

When RTACS becomes operational, the DCAOC will assume full operational control of all DSCS satellite networks. The SATCOM network control functions will be relocated to the DSCSOCs installed at host earth terminals. The DSCSOCs will be under the opertional control of the DCAOC, and will exercise the day-to-day operational direction of the DSCS. Operational plans call for a four satellite deployment, each satellite supporting between 40 and 60 earth terminals, and 150-200 individual accesses or trunks. Two DSCSOCs will be deployed at geographically disperse sites as shown in Figure 3, one operating as an "on-line" DSCSOC and the other as a "hot-standby" DSCSOC. At the DSCSOCs, SATCOM network controllers will be responsible for network operations and performance on a continuous basis. They will be assisted by a satellite controller who will monitor the DSCS III satellites and control the onboard communications subsystem configuration. The DSCS III satellites will have X-band TT&C, so that control of the communications subsystem can be exercised by the satellite controller. In addition, the DSCS III satellites are equipped with S-band TT&C for use with the AFSCF S-band TT&C capability, hence providing a backup to the X-band.

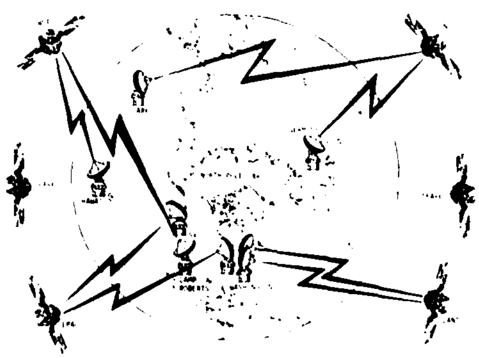


Figure 3. DSCSOC Sites

RTACS CONTROL ARCHITECTURE

The RTACS distributed processing concept is shown in Figure 4. There are three major types of functionally oriented control elements and interfacing subsystems. The control elements will be designed for installation into existing or planned DSCS facilities. These elements include the Network Control Element (NCE) of which eight are required, the Terminal Control Element (TCE) of which 150-200 are needed and the Operational Control Element (OCE) of which some twelve will be required. The DSCS Control Interfaces are shown in Figure 5.

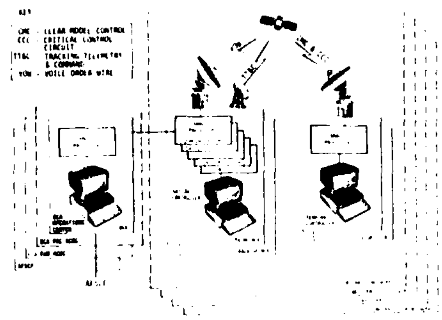


Figure 4. RTAC Distributed Processing Concept

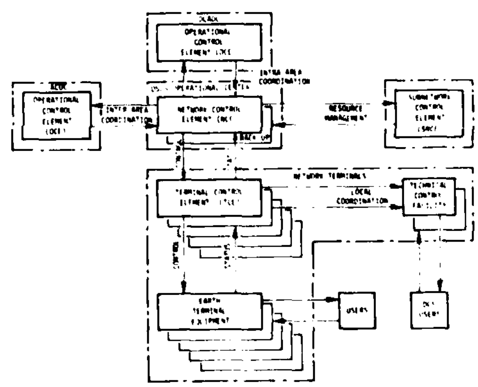


Figure 5. DSCS Control Interfaces

DSCS Operations Centers (DSCSOCs) will each be equipped with a NCE to implement the network operations and satellite control and signal monitoring functions. Network Terminals (NT's) will be equipped with TCE's appropriate to their terminal equipment configuration. OCE's will be implemented at the DCAOC, the ACOCs, and the AFSCF to provide Controllers with network control and display interfaces. In addition each Special User Network Control Terminal will incorporate an OCE as part of the Subnet Control Element Configuration for control and display functions relating to its complement of terminals.

Network Control Element (NCE)

The NCE is the central control point of the DCS control segment. It provides the SATCOM Network Controller with near-real time visibility and control of the assigned DSCS assets. The NCE consists of six subsystems.

a. A Network Control Processor (NCP) which provide computational data base management support and software maintenance support for all Net Control Elements.

b. A Controller Interface Subsystem (CIS) which provide for the real-time interactive man-machine interface between the SATCOM Network Controller and subsystems of the NCE.

c. A Satellite Configuration Control Element (SCCE) which provides the Satellite Controller full-time control and status monitoring of DSCS III satellite payload configuration via an X-band TT&C system.

d. A Signal Monitoring Subsystem (SMS) which provide surveillance and calibration of all satellite signals.

e. An Intermediate Frequency and Radio Frequency Interface Subsystem (IRIS) which provides interface control and subsystem connectivity between the Network Control Element and earth terminal equipment including up/down conversion between baseband and radio frequency.

f. The Baseband Interface Subsystem (BIS) which provides connectivity between the off-station facilities and the NCE. This subsystem includes all patching, signal conditioning, signal distribution, COMSEC, and communications test functions.

Terminal Control Element (TCE)

The TCE's provide the means for configuration control, status monitoring, performance assessment, and operator support for all DSCS transmission equipment and subsystems at each Net Terminal. The TCE interfaces directly with terminal equipment, with the local terminal operator, with the local DCS station controller, and provides control connectivity to the SATCOM Network Controller and the NCE (and back-up NCE) via a control orderwire subsystem (COSS) and the protected Critical Control Circuit (CCC). Four types of TCE's are defined to match the wide range of terminal configurations.

Operations Control Element (OCE)

OCE's provide the man-machine interface between SYSCON, SATCOM, terminal and subnet controllers. The OCE will be designed as a standard modular, stand-alone element capable of being deployed into a wide range of facilities where operational control personnel are located. Each OCE can access up to four SATCOM networks via either dedicated or AUTODIN II compatible communications interfaces.

EVOLUTION OF DSCS CONTROL

The DSCS Control Segment has been designed in a modular manner to facilitate the introduction of automation leading up to a full RTACS capability. The DSCS Control Segment will evolve from the largely Manual Control used for the current DSCS II satellites, through a semi-automated period when the first DSCS III Demonstration Flight Satellites are available (CY1981-82), to the build up of the RTACS starting in CY 83.

Pilot Control System (PCS) and PCS Extension

The PCS was deployed at four DSCS earth terminals during CY1977-78 to test and evaluate various control concepts including margin control algorithms, control orderwire protocols and control system performance. The PCS Extension (PCS-X) was initiated in CY1978 to provide an operational as well as test capability for earth terminals of the DSCS II Atlantic satellite network.

Satellite Configuration Control Element (SCCE)

Engineering Development Models (EDM) for the SCCE are being developed in parallel with the DSCS III Demonstration Flight Satellites (DFS) and will be deployed at the Sunnyvale DSCSOC for the East Pacific satellite and the Ft. Detrick DSCSOC for the Atlantic satellite during CY1981-82. The SCCE is an X-band TT&C system that will monitor and control the communication subsystem (including the multiple beam antennas) on-board the DSCS III satellite.

Control Coordination Subsystem (COSS) and AN/USC-28 Spread Spectrum Modulation Equipment (SSME)

The COSS will provide secure demand access digital voice and data services between the earth terminals in each DSCS network and a Clear Mode Control (CMC) orderwire The COSS is scheduled to be operational in CY1982. The AN/USC-28 includes an A/J protected Critical Control Circuit (CCC) that will provide a stressed condition orderwire capability.

DCSC Operational Support System (DOSS) and Resource Allocation Software (RAS)

The DOSS will provide a computational capability at the Sunnyvale and Ft. Detrick DSCSOCs to support initial testing and then DSCS operation for the DSCS III Demonstration Flight Satellites. The DOSS will be deployed with the EDM-SCCEs. The DOSS provides both local SATCOM Network Controller control as well as remote operation through operator stations at the DCAOC and ACOCs. The Resource Allocation Software (RAS) will operate in the DOSS computer and will perform the functions of Scenario Definition, Resource Allocation, Network Performance Prediction, Report Generation, and Data Base Management. The RAS provides the SATCOM Network Controller with rapid configuration plans in response to changing DSCS traffic or changing network conditions. DOSS/RAS will generate commands for the DSCS III satellite that will be sent via the SCCE at X-band, commands for the DSCS network terminals that will be transmitted via orderwire, and predicted signal parameters that will be used by DASA (see below).

DSCS Automatic Spectrum Analyzer (DASA)

The DASA will be deployed with DOSS at the Sunnyvale and Ft. Detrick DSCSOCs and will operate either with DOSS or in a stand-alone mode. DASA provides a signal monitoring capability that reduces the current monitoring time-line by a factor of 15 while using improved estimation algorithms that include the effects of intermodulation products, adjacent channel interference, and the SAW filter characteristics. DASA compares measured signal parameters with predicted values and generates alarms when the difference exceeds operator-specified thresholds.

RTACS

The U.S. Army Satellite Communication Agency is currently conducting a competition for the first phase of RTACS. This phase will be performed in CY1981-82 and will include complete hardware and software design specification as well as the development of a Software Development Facility to develop the RTACS which is an extensive software program. The second phase of RTACS will commence in CY1982 and will include the production of the NCEs, OCEs and TCEs, the deployment of these elements and contractor provided operation and maintenance support.

CONCLUSION

This paper has described the evolution of the DSCS Control Segment from the current to the planned RTACS of the 1980's. This evolution will provide improved capacity, availability and responsiveness for DSCS users while providing an orderly transition plan.

REFERENCES

1. Witherspoon, J.T., "Real-Time Adaptive Control for the Defense Satellite Communication System," Page 25.2; International Conference on Communications, June 12-15, 1977, Chicago, Illinois.

2. "Concept of Operation for the DSCS Operations Control System:, 31 January 1980, Draft.

BIOGRAPHY: P. Jeffrey Bogert is Department Head, Satellite Network Control at Stanford Telecommunications Inc. (STI). Mr. Bogert has led STI contract work with DCA in 1) Specification of the Real-Time Adaptive Control System (RTACS), 2) The DSCS Operational Support System (DOSS) and 3) The Resource Allocation Software (RAS). He is currently working on a network control study for AFSATCOM under contract with the USAF Headquarters Space Division.

Prior to joining STI, Mr. Bogert was the Program Manager of the Telecommunication System Program for System Control, Inc of Palo Alto, Ca. There he led studies for the Navy FLTSATCOM program, the DCA System Control (SYSCON) program, and the NATO Integrated Communication System (NICS).

Mr. Bogert was with the Bell Telephone Laboratories from 1963 to 1974 where he worked on the Army Ballistic Missile Defense System, the NASA Apollo Program, and Network Control and Fault Monitoring for the Bell System.

Mr. Bogert holds a BSEE degree from Cornell University, and a MSE degree from the University of Michigan.

SYSTEM CONTROL CONSIDERATIONS FOR NEXT GENERATION DCS SWITCHES

John W. Guppy, Jr.
The MITRE Corporation
Bedford, Massachusetts

ABSTRACT: System control has assumed greater importance in military long-haul communications with the increase in size and use of common-user networks. Little consideration was given to system control during the design and development of the existing DCS switches largely because of the other problems that had to be considered in order to insure a useful system. In the next generation of DCS switches, system control considerations will be a significant factor in the selection of the switches. Some of the system control considerations that should be taken into account in the selection process are discussed.

INTRODUCTION

During the last thirty years, major improvements have occurred in long haul telecommunications systems, both military and commercial. These have resulted in greatly improved service, lower costs, and increased reliance on these systems. The growth in traffic caused by the increased reliance on these systems has led to more complex networks and a greater need for system control to keep them operating at maximum effectiveness. This need is especially great in military networks where survivability in the event of a crisis is extremely important.

System control for the Defense Communications System (DCS) must take into consideration all aspects of the system. This includes both dedicated and switched service, various types of transmission media, and the various switches. While all of these aspects must be considered when exercising system control, it is possible to consider individual areas when considering what features are required in those areas for the providing of system control.

This paper will consider the features that are desirable in the next generation of DCS switches for switched voice service. The exact nature of these switches is not

known at this time nor is the time phasing of their introduction into the DCS. It is possible to make some assumptions about the nature of these switches, however.

Assumptions

The following assumptions have been made about the next generation of voice switches for the DCS:

1) Switches will be stored program with processor control;

2) Switches will employ time division digital circuit switching;

3) Switches will be compatible with both analog and digital transmission facilities;

4) Switches will handle existing signaling and supervision and also be able to work with common channel signaling;

5) Initial procurement will occur within ten years.

From a system control point of view, the most important of these assumptions is the first one. Without stored program processor control, the cost of providing system control functions in a switch is prohibitive except for the simplest functions.

Considerations

The exact functions provided for system control in the next generation of DCS switches will depend on the design of the switches and the network plans. Regardless of the details, the features to be considered can be divided into three major groups. These are those designed to minimize the need for system control actions, control actions, and status reporting to provide the controllers with the data required for control.

MINIMIZATION CONSIDERATIONS

Network congestion, actual or potential, is a basic reason for initiating a system control action. Any switch design should take into consideration those factors that could be incorporated that would tend to reduce network congestion from either heavy traffic or the loss of part of the network. There are several such factors to be considered.

Switch Processing Capacity

The switches should be designed to insure that they have adequate processing capacity during periods of congestion. In determining the required capacity, such factors as the increase in the number of preemptions and number of unsuccessful call attempts during congestion must be taken into consideration. Ideally, the speed of processing a call should not be affected by the load being carried by a switch. This ideal probably cannot be reached but it should be possible to come quite close to it. Such factors as checking additional trunks before finding an idle one or having to go through preemption processing more often during congestion contribute to not reaching the ideal.

Two areas in particular require consideration with circuit switching. These are glare and preemption. Glare is the condition that occurs when two switches simultaneously seize a trunk between them for the completion of a call. If one or both of the switches recognizes the condition, one or both may back off and try another trunk for the call. The calls are delayed by the period required to recognize the glare condition and the back off and retry. This adds to the processing load which adds to the congestion. If neither switch recognizes the glare situation, the calls can be left "high and dry" or the calls may be connected together. In either case, all of the processing for call will have been wasted and the retries of the calls will increase the congestion.

Preemption can present an even more serious situation than glare. If a portion of the switch logic is tied up during the preemption process, as is the case with the existing Overseas AUTOVON switches, this logic cannot be processing other calls at the same time. With the existing AUTOVON preemption arrangement, the reduction in

switch capacity when a considerable number of preemptions occur is significant as the operation during which preemption occurs goes from 200 milliseconds to over 700 milliseconds.

The glare and preemption problems can be minimized by the use of a properly designed common-channel interswitch signaling arrangement. The use of logic operating at a considerably higher rate than that required for the normal traffic load will minimize the delays in the basic call processing during periods of congestion.

Ineffective Preemptions

Ineffective preemptions occur when an interswitch trunk is preempted for the setting up of a call that is later blocked by calls of a higher precedence or equipment problems. These ineffective preemptions result in additional congestion when the preempted calls are replaced. Ineffective preemptions can be a particularly serious problem on trunk groups leading to switches that serve as gateways to other areas. This is the result of the high probability of blocking on the high-usage interarea trunks.

Common channel signaling arranged so that no preemptions occur until it had been determined that the desired connection can be set up would reduce the number of ineffective preemptions greatly. Some changes in the way in which a trunk is selected for preemption may also be required if the existing arrangement of two types of trunks, voice and special grade, is retained in the future.

Release Trunk Centralized Assistance Operators

Assistance operators in the DCS have been centralized in many areas in order to make more efficient use of personnel. When an assistance operator extends a call, this can result in inefficient use of transmission facilities because of poor routing. It can also result in the operator having to place two calls, one back to the originator and one to the destination to upgrade the precedence of a call. The inefficient routing is undesirable at any time, and especially undesirable when congestion exists. Having to place two calls for a precedence upgrade can contribute to congestion by slowing the operator response to another call.

Released-trunk operation of calls to assistance operators would reduce both of these problems. This type of operation could be provided in either of two ways. The first would be to provide special trunk groups to the centralized operators. With this arrangement, all calls for the assistance operators would be routed over these special trunk groups. When the operator extended a call, the appropriate instructions, including precedence upgrade would be routed back to the originating switch which would then set up the call as if it had been originated locally with the exception that no checks would be made to insure that the originators class marking allowed the call. The trunk to the assistance operator would then be released. The second approach would set up the connection to the operator using a regular trunk arranged for common-channel signaling for the connection to the operator. The operators instructions for the handling of the call would then be sent back to the originating switch using the common-channel signaling along the route of the call. The switches along the route could then determine at what point the connection to the operator should be dropped and a new connection established. Precedence upgrades would be transmitted back to the originating switch to permit all switches involved to store the new precedence.

The use of special trunk groups is less efficient than the use of the regular trunks and common channel signaling. The special trunk groups offer the advantage of not competing with high precedence traffic for trunks. This could be of considerable importance in situations where a precedence upgrade is required.

CONTROL CONSIDERATIONS

System control actions are provided for minimizing congestion, minimizing the impact of facility losses and handling interconnections with other systems established to handle special situations.

Routing Changes

The DCS makes extensive use of alternate routing to handle traffic peaks and to provide routing around trouble spots. There are conditions such as congestion and severe outages where the extensive use of alternate routing can actually make the problem worse.

Provision is needed for making routing changes in a rapid and efficient manner.

The present arrangement in the Overseas AUTOVON switches is limited to cancelling alternate routing to a destination or blocking all calls to a destination, i.e., code cancellation. The present method of implementing the changes is awkward and slow and needs improvement. In addition, it would be highly desirable to have a more flexible arrangement that would permit the cancelling of individual routes including the first choice route. This would be very useful when a problem occurred on the first choice route but not on the alternate routes.

Partial route cancellation where a route was cancelled for all calls below a given precedence would permit high precedence calls to take advantage of alternate routing but restrict the routing of low precedence calls.

Code Cancellation

Code cancellation is a form of routing change in the existing DCS in that it is implemented by cancelling all routes to a given office code or group of office codes. When a call is placed to a code that has been cancelled a unique announcement is given to the calling party. Expansion of this function to permit code cancellation for low but not high precedences would permit limiting calls to high congestion points without completely cutting off service. This would be very useful in restricting the calls to selected office codes working in a switch when the congestion was largely the result of calls to the PBX's assigned these codes.

Automatic code cancellation for four-wire lines and for PBX's where all of the access lines have failed would be desirable. This would be provided only at the switch providing service to the four-wire line or PBX and would result in the special announcement being returned if the four-wire line or all of the lines to the PBX had been out-of-service for at least a minimum specified time. This would delay or prevent retrys of calls that would be made if a busy tone or announcement were returned as is the case at present. The minimum time element is required to prevent returning the announcement in case a call is blocked on the initial try by a short transmission fade.

Line-Load Control

The activation of line-load control prevents selected subscriber lines, including PBX access lines, from originating calls but allows them to receive calls. The present AUTOVON switches have three classes of line load control which can be used singly or in combination. When applied, line load control helps to relieve congestion by reducing the number of local call originations.

Additional classes of line load control would be desirable in order to provide finer control. If the switch design permits, it may be desirable to provide line load control in a form that allows calls above a certain precedence to be originated but not others. Another variation would be to allow calls to some destinations to be originated but not to others. This would permit limiting the traffic to congested areas from some subscribers while allowing them from others with a clear need for such calls.

Trunk Directionalization

Trunk directionalization is similar to line-load control but is used on interswitch trunks to limit them to one direction of call placement. It is used to limit the number of trunks available for calls going to a congested switch or to insure that some trunks are available in both directions between two switches. Reserving trunks for a specific direction between two switches may be necessary at time to insure that calls can be completed in that direction when precedence restrictions would heavily favor calls in the other direction.

Trunk directionalization should operate in a manner that does not reduce the call processing capability of the switch and does not result in the mishandling of calls. The existing interswitch trunk directionalization in Overseas AUTOVON can result in extra switch marker operations and can also result in a call being blocked when a trunk group is partly directionalized and there is a nondirectionalized trunk available for preemption.

A modification to trunk directionalization that would directionalize the trunk for low precedence call but not high precedence calls would be a useful control in some situations. In some situations, it would act very much like partial code cancellation. It could be used, however, to

allow some alternate routing through a congested point when partial code cancellation had been used to limit calls to the congested point.

Tactical Subscribers

Provision is being made in the DCS for making interconnections with tactical subscribers on a real-time basis. These subscribers will move around from time-to-time and the exact location where the interconnection for any given tactical group will be made cannot be predicted in advance. Efficient operation requires that the telephone numbers assigned to these subscribers be independent of the point of interconnection.

This requires that the DCS switches be capable of rapid programming for the routing of calls to these subscribers. It would be very desirable to have a single message, entered at the point of interconnection, to automatically distribute the routing information throughout the network. This would not be difficult to provide with common channel signaling.

Class Mark Changes

During a crisis situation, the importance of a given four-wire telephone or PBX may change greatly. This makes it highly desirable to be able to change the class markings of individual lines rapidly when necessary. The class markings of most interest are the precedence limit and allowed calling area. Those markings associated with such things as type of signaling required are of less importance but the ability to change them rapidly in case of restoration with a different type of equipment would be useful.

Circuit Activation

Provision for activating reserve transmission facilities would be very desirable if such facilities may be provided in the future. These could be military facilities that had other uses in a noncrisis situation or be circuits leased on a standby basis. At the present time, there is no provision in the Overseas AUTOVON switches for this type of operation and no such circuits.

REPORTING FUNCTIONS

The reporting functions can be divided into physical status and traffic reporting. Both of these are important from a system control viewpoint.

Switch Status

The system controls require a knowledge of the physical status of the switch at all times presented in a form that indicates the call handling capability of the switch. The exact data required will depend on the details of the switch design. Experience with the present Overseas AUTOVON switches has shown that it is essential that the data provided be as unambiguous as possible. Of particular importance is that routine maintenance and operational acts do not appear to the system controllers as potentially serious trouble conditions.

Transmission Facility Status

The switch is in a position to identify certain transmission problems that cannot be readily identified in any other manner. In particular, problems associated with the signaling units on analog trunks and lines and the cross-connections between the transmission facilities and the switch with both digital and analog facilities can be readily noted by the switch controller. Exactly what the switches should report in the way of transmission facility status will depend on the state of automatic monitoring and reporting in this area by other means and the degree of integration provided in the areas of transmission and switching.

Traffic Reporting

The switches will have to provide for traffic reporting for both system control and long-term engineering purposes. For system control purposes, information of the number of calls being processed, loading of various trunk groups, and the amount of blocking occurring will be required as a minimum. The reporting interval used must be long enough to minimize the effect of the random nature of the traffic but short enough to be meaningful for real-time control. A moving window type of reporting would be desirable to permit rapid determination of the effect of control actions.

CONCLUDING REMARKS

The system control considerations covered in this paper almost certainly do not include all of the considerations that should be taken into account. Special features and services may be introduced into the DCS that will introduce system control needs that are not evident at the present time. Such factors make it essential that the system control considerations for the next generation of DCS switches be continuously updated with changes in the DCS as they are planned and implemented.

One possible consideration, channel reconfiguration, has been deliberately left out. This function would be useful in switches to which subscribers were rehomed in the event of a switch failure. At a failed switch, however, the failure of the switch could prevent the rehoming if the channel reconfiguration was performed by the switch. It, therefore, appears desirable to provide the channel reconfiguration function as a separate unit.

BIOGRAPHY: John W. Guppy, Jr. holds the position of Department Staff at The MITRE Corporation. Since joining MITRE in 1960, he has been involved in air traffic control studies, the 490L Overseas AUTOVON Switches Program and a variety of other communications programs. He is presently involved with the AUTOVON Network Control Subsystem project.

Guppy was previously a Member of the Technical Staff for Bell Telephone Laboratories, where he was engaged in special systems studies. He holds Bachelor's and Master's degrees in Electrical Engineering from the Massachusetts Institute of Technology and a Bachelor's degree in Physics from the College of William and Mary.

EVOLVING APPROACHES TO SYSTEM CONTROL IN THE DCS

Dr. L. Jankauskas & G.G. Wilson
GTE Products Corporation
Needham Heights, Massachusetts

ABSTRACT: Functions performed by System Control have become more automated to enable the controller to more rapidly assess network performance and take corrective actions. Described are some of the early approaches and systems for System Control. Characteristically these systems provide a measure of performance requirements imposed on the transmission network. Examples of such systems are Data Sentinel, Communications Performance Monitor, and Communications Circuit Equipment Switch.

With the advent of digital techniques for DCS transmission, most recently digital multiplexers and radios, a system control approach directed at reconfiguration of the network based on reassignment of digital channels in a multiplexed digital group has been evaluated and is described under Digital Network Control. Also highlighted is a network fault detection and isolation approach to operate at nodal level; an approach tested and verified by simulation on the CPMAS program. Finally, an approach, called Adaptive Channel Estimation (ACE) is described. ACE derives estimates of link/radio performance, in essentially real time, for high data rate (megabit per second) transmission.

1.0 INTRODUCTION

The methodology used to maintain and restore communication's assets to their optimum performance levels in the Defense Communications System is the function of System Control. With the changing technological advances, (LSI for hardware implementation, digital techniques, computers, and software programming) new approaches for System Control have evolved. Today, System Control facilities have evolved such that new functions not originally provided can now be provided because complex functions and algorithms, such as fault isolation of communication problems, can be implemented in software. Automation of these processes pro-

vides greater real-time control of digital and analog traffic in response to changing operational conditions.

2.0 INITIAL APPROACHES

The evolutionary process began with analog and manual techniques for system control. Next in the process was replacement of analog techniques with digital techniques, encouraged with the advent of integrated circuits. For both of these cases, control was accomplished by manual assessment of one circuit at a time. This was changed, in the next evolutionary step, by adding a hard-wired capability to automate the process of monitoring by using sequential scanners to connect circuits to be tested to one central analyzer. To some extent, the reporting of measured results was also automated. Table 1, Terrestrial System Control Evolution identifies the various stages. As an example, low speed digital circuits were once tested with an analog device presenting a circular display calibrated in the baud interval to present a measure of bit distortion to the operator. Operator control was a matter of adjusting loop current to correct for the distortion or bypassing the circuit through manual patching at the DC jack field. System control has advanced to the point now where automated patching is under consideration at the 1.544 mb/s digital group level, discussed later under Digital Network Control.

Using measurement of the DC-circuit as an example, the analog measurement approach was replaced with a digital approach, and eventually digital integrated circuits were used to make performance measurements. Some of these test sets were nomenclatured AN/GGM-15, 16 or 17, Digital Distortion Test Sets. The time frame was in the mid-1960s. In more recent systems, such as the Communications Performance Monitor (CPM) for the NORAD Cheyenne Mountain complex and the Automated Technical Control (ATEC) system, this function is implemented with software. In the earlier systems a tech controller would patch into a circuit, one at a time, and read a digital display of various types of distortion. In today's systems the information is presented on a video display terminal, information being obtained from a data base.

Table 1. Terrestrial System Control Evolution

. Manual measurements of circuit performance characteristics one circuit at a time	. Analog techniques . Hard-wired logic . Manual system control	. Various analog test equipment
. Introduction of digital technology to replace analog technology	. Digital techniques . Hard-wired . Manual system control	. AN/GGM-15 series (digital distortion measuring set)
. Introduction of automated sequential scanners to connect many circuits to one central circuit analyzer	. Digital techniques . Hard-wired . Some automated monitoring	. Access . Data Sentinel
. Introduction of computer to aid in quality monitoring and reporting	. Automatic	. AQMRS . ATC (semi)
. Upgrade of tech control facilities and off-line circuit testing	. Analog-to-digital . Manual	. WWTCIP
. Computers used to replace analog and digital in-service monitoring and assessment measurements	. Computerized	. ATEC . CPM . CPMAS
. First major automated patch capability	. Hard-wired switching under computer control	. CCES
. Automated patching/channel reassignment approaches evaluated	. Automated . Computer controlled	. CRM
. Advances made in link/performance assessment and fault isolation	. Automated . Software/firmware	. CPMAS

The addition of sequential scanners decreased the time to take circuit measurements. In the late 60's, one of the first systems to use this approach was the Automatic Communication Circuit Evaluation and Sensory System (ACCESS). Today's systems use the same concept, the major difference being earlier systems were designed with hard-wired logic and with manually selectable strap-options based on the type of circuit being tested; whereas today's systems are computer controlled with options set in the data base through a terminal device (VDU, tape, etc.).

In the same time frame, one system, the Automated Quality Monitor Reporting System (AQMRS) was installed at Coltano, Italy and another, Automated Technical Control (Semi)-ATC (Semi) was installed in CONUS at Fort Detrick, Maryland. The AQMRS is a computer-controlled monitoring and reporting system for link, terminal, group, voice channel, and telegraph channel equipment. It alerted personnel to outages, degradations, or changes in status. The ATC (Semi) is similar to the AQMRS but has additional limited capability for semi-automated patching.

The system control approaches which evolved in about 1970 basically provided the tech controller with a capability to more rapidly access communications network operation. Functions performed by hardware and/or software were generally limited to providing data concerned with the technical parameters of the circuits and equipment; e.g., measurements of analog level, distortion, frequency, noise and the like. Corrective action, based on the tech controller's capability to 'manually' fault isolate, was by manual patching - as it is today. One of the most recently tested concepts, to be described later, for automatic fault detection and isolation in the digital DCS backbone; has been designed and tested, by simulating fault scenarios, on the CPMAS program.

3.0 DATA SENTINEL

Commercial circuit quality monitoring systems (CQMS) measuring DC and quasi-analog circuits have also been delivered; one, for example is the "Data Sentinel" system for the Penn Central Transportation Company in Philadelphia. This system is designed to scan about 200 digital circuits and 100 quasi-analog circuits on a continuous, non-interfering basis. This system is a hard-wired system measuring the same parameters on commercial circuits as are measured on military circuits. Figure 1 shows the functional approach.

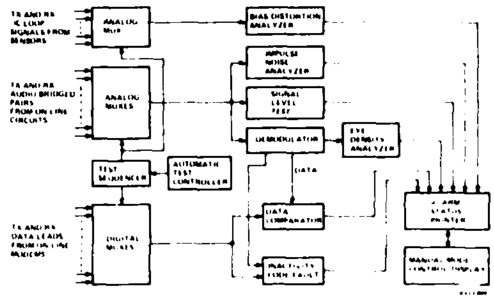


Figure 1. CQMS Functional Block Diagram

Distortion is measured on each transmit and receive digital circuit by the 'bias/distortion analyzer' as each circuit is multiplexed through the 'analog mux'. Based on data printed out to the controller, appropriate corrective action can be taken. For transmit and receive quasi-analog signals, impulse noise and signal level are measured and the eye pattern of a demodulator connected to the audio bandwidth signal is analyzed for signal levels which exceed threshold levels.

In this particular application all of the modems are the same type so that an approach which uses one demodulator, in effect a test modem, is a cost effective solution for both eye density analysis and a bit-by-bit data comparison of the test modem with the on-line modems. Transmit and receive on-line digital data is connected through the 'digital muxes' for analysis. In applications having many varied modem types, manufacturers, etc., this approach may not warrant the cost, a modulator is required for each different type of modem.

4.0 COMMUNICATIONS PERFORMANCE MONITOR AND COMMUNICATIONS CIRCUIT EQUIPMENT SWITCH

A major computer controlled system for assessing communications performance is the Communications Performance Monitor (CPM) designed for operation at the NORAD Cheyenne Mountain Complex. It also includes a very large automated patching capability, called the Communications Circuit Equipment Switch (CCES). The CPM measures performance parameters of DC and quasi-analog circuits with calculations performed in software. The CPM scans about 2000 points in less than three minutes. Figure 2 shows the functional approach.

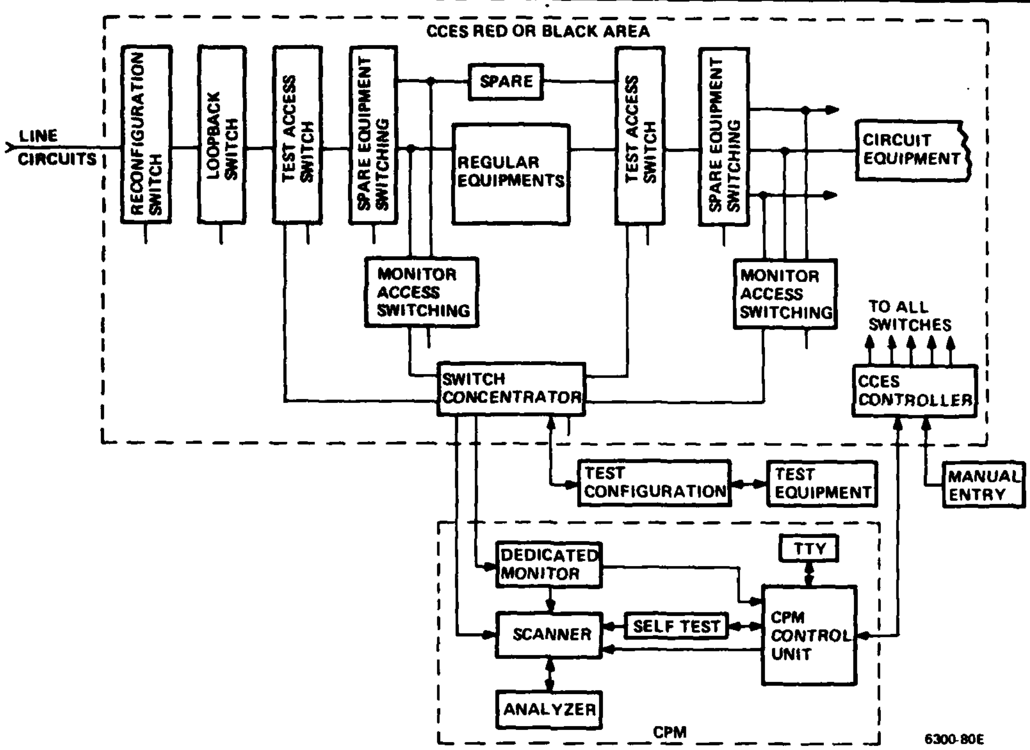


Figure 2. CPM and CCES Functional Block Diagram

The CCES, providing an automated patching capability, is organized functionally to provide:

a. A loopback capability (loopback switch)

b. Access to signals for in-service monitoring only (monitor access switching)

c. Access to equipment and circuits for off-line testing (test access switch)

d. Access to equipment handling only RED signals or only BLACK signals for purposes of switching in spare equipment (single area spare equipment switching)

e. Access to equipment handling both RED signals and BLACK signals for purposes of switching in a spare equipment (dual area spare equipment switching).

All switching is controlled by a CCES Controller which is provided information from the processor or from a manual entry panel which provides backup for the processor. With this organization of switching capability a controller has access, at one central location, to any point along a circuit. All points are brought to this central monitoring facility by means of a switch concentrator, which functions to allow simultaneous selection of up to any of 20 test access points or monitor access points from the total of about 2000 points. Based on results of monitoring and testing a determination is made whether or not to switch in spare equipment. Connectivity of the switches is such that one spare could be connected in place of any one of ten on-line equipments.

5.0 DIGITAL NETWORK CONTROL

Studies have been accomplished regarding an approach to improve network reconfiguration and flexibility in a network using time division multiplex equipment. One such method, called Digital Network Control (DNC) is based on the concept shown in Figure 3. DNC is a form of channel reassignment and denotes the ability to assign data in a time slot of a digital group to another time slot in the

same group or into different groups. The result of a channel reassignment is equivalent to patching operation performed at the basic channel level.

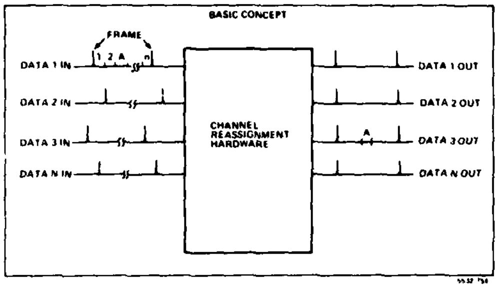


Figure 3. Basic Channel Reassignment Concept

However, the advantages gained by channel reassignment as opposed to patching are:

a. The operation can be remotely controlled.

b. The operation can be performed at stations where there is no channel breakout and thus where channel patching is otherwise not possible.

c. Several channels or a group can be reassigned as rapidly and as accurately as a single channel.

DNC also provides operational benefits other than related to system control. These include rapid restoration of high priority circuits, provision of means for DCS transmission control to perform performance assessment and fault isolation in digital circuits and the ability to automate some tech control functions at unattended stations.

Based on analyses the location within the digital hierarchy in which the DNC should be integrated was determined to be at the digital group level as shown in Figure 4.

Although the DCS digital formats are byte-interleaved, an implementation approach which can accept bit-interleaved digital data, as is used in TRI-TAC, is suggested. Figure 5 indicates such a modulator approach. The DNC A function performs reassignment of byte-interleaved channels; DNC B, of bit-interleaved channels. Either function should be capable of stand-alone operation.

6.0 CPMAS (Abstracted from Reference 1)

In order to be responsive to the monitoring and performance assessment requirements of a mostly digital DCS, the Communications Performance and Assessment for DCS Digital Systems (CPMAS) program was undertaken. The CPMAS program has developed an emulation facility on which the present fault detection/isolation algorithm, and other new algorithms, can be tested in a controlled environment.

The status monitoring and performance assessment functions are performed by two processors, the Adaptive Channel Estimator (ACE) and an LSI 11/03, the composite being referred to as the CPMAS-D (D for digital) unit. When the software residing in the CPMAS-D unit detects a monitor point transition (alarm to/from non-alarm) it transmits the monitor point information to the CPMAS Emulator, a PDP 11/60 minicomputer. These messages, called exception reports, enable the CPMAS Emulator to perform its prime mission; fault isolation. Figure 6 shows the equipment comprising the CPMAS emulation facility. The CPMAS emulator, namely a Digital Equipment

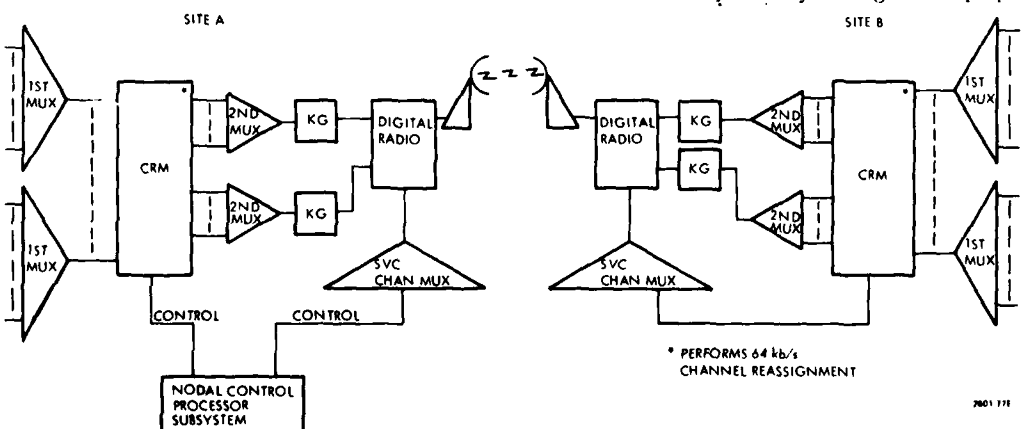


Figure 4. Digital Network Deployment

Corporation (DEC) PDP 11/60 and associated peripherals performs the nodal and sector level technical control functions. The two CPMAS-D units, including the ACE units, perform the station level technical control functions. Monitor point simulators provide simulated monitor point status, which is scanned by the CPMAS-D units. Two VIDAR T1-4000 multiplexers operating at 12.5526 Mb/s provide the ACE units with signals to be monitored.

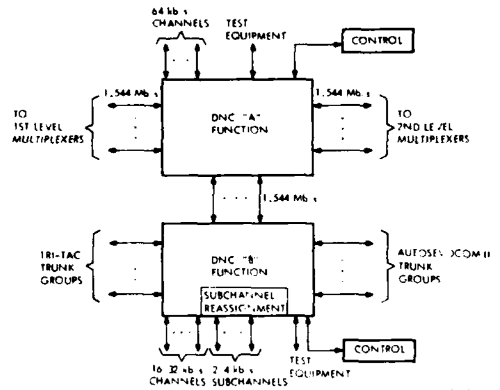


Figure 5. Digital Network Control Functional Modularity

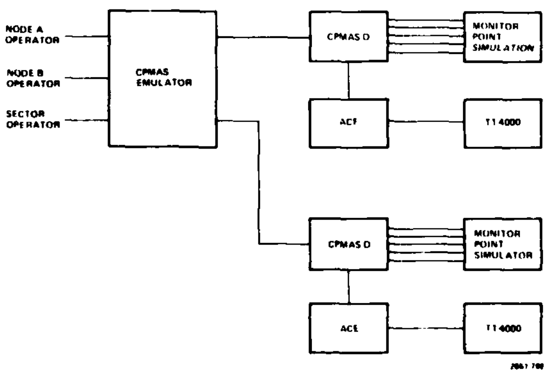


Figure 6. CPMAS Demonstration System

The primary function of the CPMAS Emulator is the execution of the CPMAS fault detection and isolation algorithm. The detection and isolation of faults in a DCS communications network is complicated by the generation and propagation of sympathetic alarms. Sympathetic alarms propagate downstream from the real fault following the network connectivity and hierarchical structure and are triggered at non-faulted equipment as a result of signal anomalies caused by faulted upstream equipment. The function of a fault detection/isolation algorithm is to locate the faulty equipment by discarding the sympathetic alarm reports.

The CPMAS-D Unit, exclusive of the ACE unit, performs the station level CPMAS functions of performance monitoring, performance assessment, and telemetry. The CPMAS-D monitor interface function monitors binary alarms, analog parameters, pulse parameters, and ACE parameters by a sequential scan technique. Performance assessment consists of the detection of changes in alarm state or threshold crossings.

The ACE operates as a major component of the CPMAS-D unit. The ACE provides a means of measuring the quality of microwave line-of-sight radio links employing either three-level partial response or quadrature phase shift keying modulation techniques.

The monitor point simulator provides the signals which drive the CPMAS-D unit performance monitor function. These signals are binary alarms which represent hard transmission equipment faults, analog voltages, intermittent binary signals (pulses), and radio baseband signals which represent performance monitor parameters. These are thresholded to assess the performance of the transmission equipment and/or network.

6.1 Fault Detection/Isolation

The inputs to fault detection/isolation are equipment status (either via station emulation or CPMAS-D exception reports) and network connectivity. The global approach used by the algorithm examines in one cycle the entire network status, including all alarm monitor points, and simultaneously locates all faulty equipment.

The CPMAS fault detection and isolation functional flow is shown in Figure 7. It consists of five phases. First, exception reports or emulated status are received and acknowledged by the algorithm. These reports are used by the algorithm to maintain the current status of all equipments via an Equipment Status Table.

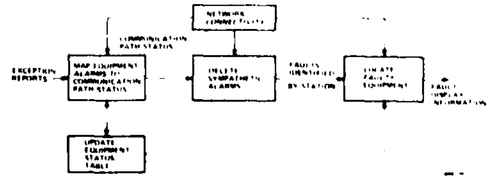


Figure 7. CPMAS Fault Detection/Isolation Approach Functional Flow

The second step maps the equipment alarms into their effect upon each communication path which is described in terms of its hierarchical transmission structure (supergroups, groups, and channels). For any station each unit of equipment (e.g., radios, second level multiplexers, etc.) is associated with a unique position within this structure. The Equipment Status Table preserves this information thereby enabling the algorithm to map the equipment alarms into a communication path status for each station. The status is represented as either a non-alarmed (in service) or an alarmed (out-of-service) state.

The third step is to delete the sympathetic alarms. The hierarchically described communication path status for each station and the network connectivity are the inputs to this function. The output is a list of stations with real faults. All downstream alarms at the same or lower level from the real fault are classified as sympathetic alarms and deleted. The faults identified by this interim process are described in terms of a station name and a position on the communication path hierarchy. The fourth step determines the equipment corresponding to each real fault. This process consists of scanning the Equipment Status Table for the alarmed equipments at the hierarchical level and station reported as faulted.

The final step is to display the network faults to the Technical Controller. The prime output is a list of all network faults with each identified to the faulty equipment.

The main advantages of this algorithm is its global network approach and fault isolation speed. The global solution is characterized by locating all network faults during each pass of the algorithm. This parallel processing is enabled by a design which describes faults in terms of their communication path status rather than in terms of equipment faults. The algorithm systematically examines the entire network to delete sympathetics using bookkeeping procedures which delineate all independent real faults. The fault isolation time is reduced in two ways. First by using the parallel approach all faults are isolated simultaneously. Moreover, the communication path status reduces the bookkeeping and allows highly repetitive and efficient processing.

The CPMAS fault detection/isolation algorithm has been extensively tested using the station emulation capability previously described. These tests demonstrated that the algorithm can successfully isolate single and multiple faults and performs independent of alarm arrival order. The fault detection/isolation algorithm successfully isolated the faulty equipment for all tests conducted. To demonstrate that fault isolation time is insensitive to fault loading, independent channel and group faults were injected using the station emulation function. The results for a 16-station model network partitioned into three star networks are presented in Figure 8. As shown in this figure, the fault isolation time is essentially independent of the number of independent faults or their hierarchical level.

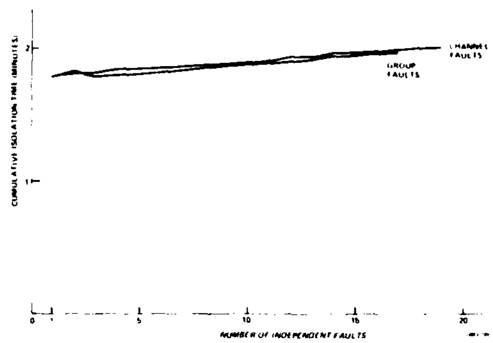


Figure 8. Fault Isolation Time (Model Network)

6.2 Adaptive Channel Estimator

The planned transition of the Defense Communications System (DCS) from an analog FDM/FM system to a digital PCM/TDM system has created the necessity to develop performance monitoring techniques that are applicable to the all-digital world. It is desirable to monitor the transmission system in such a manner that data transmission is not interrupted, while being able to alert the technical controller of a fault prior to the onset of serious system degradation. The adaptive channel estimator (ACE) unit was developed on the CPMAS program to meet the need for a fast and accurate performance monitoring technique applicable to digital transmission systems.

The ACE unit applies adaptive estimation techniques by adaptively estimating parameters that can be related to error rate. The basis of the algorithm is that under low error rate conditions the detected data sequence is an accurate representation of the transmitted data sequence and by using adaptive processing techniques channel characteristics can be identified.

An Adaptive Channel Estimator (ACE) field test was conducted at the RADC test facilities from 6 November, 1978 to 23 January, 1979. The purpose of the ACE field test was to gather the data necessary for an evaluation of the ACE development unit as a means of assessing performance of high-speed digital radio transmission systems.

The results of the field test demonstrate that the ACE unit can be used over a variety of operating conditions and can effectively assess performance of digital communications systems. For the T1-4000 tests, the ACE unit was able to accurately estimate the counted bit error rate (BER).

REFERENCES

1) L. Jankauskas, M. Landesberg, D. Spector, and C. Meyer, "Technical Control of the Digital Transmission Facilities of the Defense Communications System," IEEE Trans. on Communications, Sept. 1980.

BIOGRAPHY. George G. Wilson is Manager of the Switching and Control Systems Department of GTE's Communication Systems Division in Needham, Mass. Since joining GTE in 1973, he has led activities related to research, design, and development of Systems Control and Technical Control for analog and digital networks. He has been an engineering task manager and lead systems engineer for Communications Performance Monitoring and Assessment (CPMAS) program for RADC, Digital Network Control (DNC) study for DCEC, Supervisory Control System (SCS) studies for NAVELEX, Communications Performance Monitor (CPM) System for NORAD's 427M Technical Control Facility and Penn Central Performance Monitoring System. He has also performed studies and proposals for ATEC, TRI-TAC's TCCF, NAVACCS, SATCOM III and SVIP.

Prior to joining GTE, Mr. Wilson held the position of Engineering Manager for military programs directly upgrading Technical Control Facilities. These programs included both circuit and equipment quality monitoring systems, VF and DC line conditioning equipment, timing recovery systems and other related elements.

Mr. Wilson has a Masters Degree in Mathematics from Adelphi University and in Electrical Engineering from Worcester Polytechnic Institute. He is a member of Eta Kappa Nu and the author of several published papers.

BIOGRAPHY. Louis E. Jankauskas is an Engineering Specialist at GTE's Communication Systems Division in Needham, Mass. Since joining GTE in 1975 he has been engaged in research and development in the areas of performance assessment, fault isolation, system control, secure voice, and signal processing.

From 1973 to 1975 Mr. Jankauskas worked for CNR, Inc., where he analyzed performance assessment and system control approaches. From 1969 to 1970 he worked for Western Electric Company on the SAFEGUARD program and from 1966 to 1968 he examined satellite system performance at Hughes Aircraft Company.

He received a B.S.E.E. degree from Newark College of Engineering in 1966, a M.S. degree from UCLA in 1968, and M.A. and Ph.D. degrees from Princeton University in 1973. He is a member of the IEEE Communications Society.

NETWORK CONTROL AND THE CRM MAKE POSSIBLE AUTOMATED DIGITAL PATCHING

A. Argenzia
Rome Air Development Center
Griffiss Air Force Base, New York

R. Crowe, R. Krzyzanowski, B. Simmons
Systems Research Center
Honeywell Inc.
Minneapolis, Minnesota

ABSTRACT: The digitization of the DCS has created an opportunity for the automation of Network Control functions. A Channel Reconfiguration Model (CRM) will provide full channel-level reassignment of DCS station traffic. This device will be under the remote control of an automated Network Control system. This system will monitor network status reports and utilize the CRMs to route traffic around reported faults. This paper discusses concepts employed in a feasibility demonstration of CRM and Network Control which Honeywell is currently developing.

Transmission Network Control is the element of System Control which assures that required circuits are installed and operating whenever sufficient transmission resources are available. Currently transmission Network Control is a highly manual, decentralized process. Technical controllers at each node coordinate via teletypes and telephones and use patch cords to make temporary connections to restore service. Distribution frames are rewired to make permanent connection changes. When interconnection between dissimilar systems is required, it is now done in the analog domain at a channel level.

The change to a digital transmission system makes possible remotely controlled electronic patching devices. Adding performance monitoring data and a telemetry net to collect that data and to distribute control actions to the patching devices, automation of the Network Control function becomes possible. Both temporary restorals and permanent reconnections can be made using this equipment. The electronic patching can also provide transmission inter-

connection between dissimilar networks with a bit of digital processing.

Automation can evolve from simply giving the controller computer driven CRT displays and allowing manual path selection to an entirely automated routing process. The entirely automated routing process allows the transmission network to adapt to changing demands automatically - just as the switched networks do. Achieving verified performance and user acceptance is the hurdle in implementing this totally automated system. A robust control system with a reliability and survivability equal to that of the transmission network itself is essential in leaping that hurdle. (A companion paper from DCEC will address this subject.)

Steps in automating Network Control are being taken at Honeywell, under contract to Rome Air Development Center. Honeywell is developing feasibility demonstration models of the electronic patching devices - called Channel Reconfiguration Models (CRM). These are, in essence, digital telephone switches without the call processing, signalling and supervision. What makes these units special is their compatibility with T1 and TRI-TAC and their modularity. That modularity makes it possible to adjust them to the size of a site and to add other interfaces by a module replacement - interfaces such as NATO digital trunks, level 2 multiplex streams, satellite system interfaces, and digital subchannels.

Honeywell, under contract to the Defense Communications Engineering Center, is developing concepts for the overall Network Control system for the DCS in Europe and a software system to validate those concepts. This work is only a segment of the total Network Control development. The functionality of gathering data, making decisions, translating commands, and transferring them to the patching devices is being addressed.

The next step will be to develop concepts for making the Network Control system as survivable as the DCS which it controls. Initial concepts for this have been formulated. Much additional work is required to finalize this system.

The intent of this paper is to describe briefly the nature of the work to date in CRMs and in Network Control. To this end, we will describe the following facets of CRMs:

- Functional requirements
- Implementation approach
- Capabilities for further expansion.

For Network Control, we will describe:

- Requirements
- Recommended system concepts - including those to make the system survivable
- Contents of the concept validation system.

The Channel Reconfiguration Model

The CRM is the hardware which provides the automated patching of the automated Network Control system. The requirements on the CRM in this role are to:

- Interface DCS and TRI-TAC digital groups.
- Reassign any channel on any incoming group to any outgoing channel/group.
- Modify channel reassignments in response to Network Control system commands.
- Monitor internal operations and report CRM faults to Network Control.
- Monitor status of incoming digital groups.

The following paragraphs describe the implementation approach taken to meet these requirements.

The components of the CRM include the hardware which handles the communications traffic and a microprocessor which accepts control commands from the Network Control system or a local terminal (Fig. 1).

The CRM hardware carries out the actual reassignment function per control instructions from the microprocessor. The microprocessor acts as the intermediary for control of the CRM by a local terminal or Network Control system. The microprocessor has the capability to change channel reassignments in the hardware as well as monitor hardware status and activate spares when appropriate.

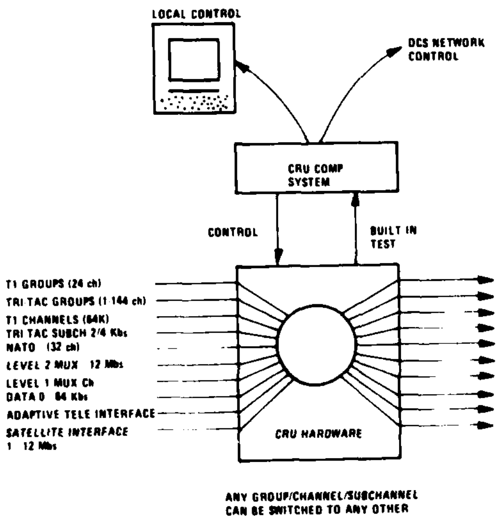


Figure 1. CRM Interfaces

The CRM interfaces digital bit streams, either as individual channels or as multiplexed groups of channels (see Figures 1 and 2). It is capable of interconnecting any pair of digital channels (received individually or in a group) in a duplex manner or in a simplex (unidirectional) manner. The CRM as is currently being developed, interfaces T1 groups and TRI-TAC groups (128Kb/s to 1536Kb/s, types 1, 2 and 4B). It also interfaces TRI-TAC channels and subchannels, and 64Kb/s synchronous channels that are analogous to those found in T1 groups. It is capable of combining TRI-TAC subchannels and channels into T1 groups.

Interoperability between networks is provided by the CRM. It can transmit TRI-TAC channels over the T1 transmission system and T1 channels over the TRI-TAC transmission system.

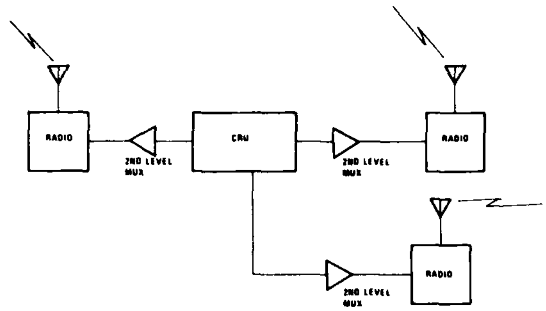


Figure 2. Channel Patching with a CRM

The configuration of the unit to be delivered in the current development supports the connections shown in Table 1. It is capable of 2880 channel level connections. The number of channels to which it interfaces is limited by the number and type of input/output cards and the particular configuration of the connected signals. Each interface port may be a single channel or a multichannel group. For TRI-TAC, the particular make-up of the group varies including 8 through 96 channel groups. The total number of channels allowable on a given 8 interface card is limited to 192 channels. Thus, the exact capacity of a given CRM depends on the consistent interfaces. The design concept for the CRM standarizes the interface to the reassignment network (inputs and outputs) as an 8-bit wide 8000b/sec, 64Kb/s rate (Figure 3). Thus, T1 and TRI-TAC both are converted to such a format and bits in excess of that required for the specific channel rate are unused. The interface card slots are universal. T1 or TRI-TAC cards can be used in the same slot. These same universal slots can also be used to interface:

- NATO
- ATACS (Current generation Army Tactical)
- Level 2 (8-T1 groups at 12.928 Mb/s).

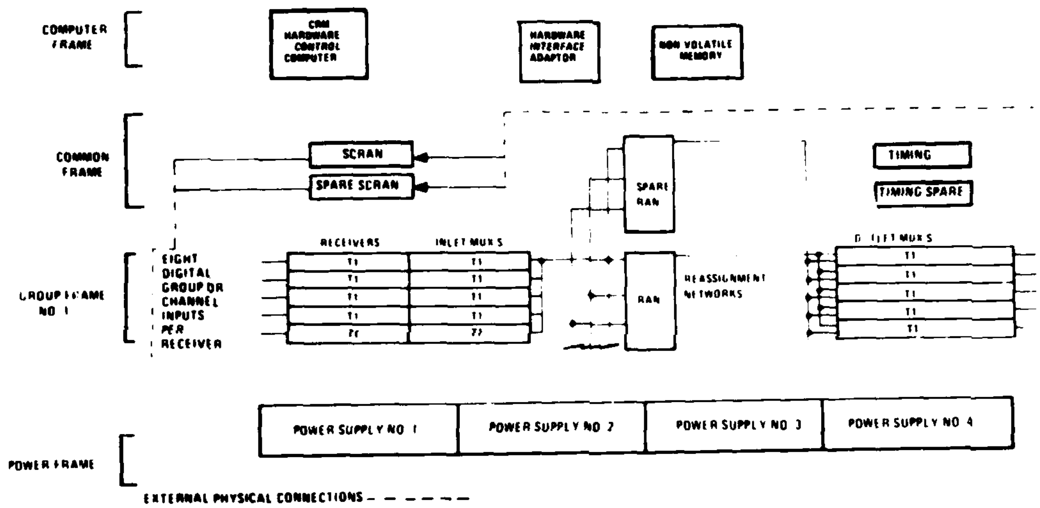


Figure 3. CRM Architecture

Table 1. Prototype CRM Interconnect Capabilities

T1	72 full duplex ports on 9 board sets. Allows channel level reassignment of up to 72 groups (72 x 24 = 1728 channels) or 72 single channel inputs.
TRI-TAC	16 full duplex ports on 2 board sets. Allows channel level reassignment of up to 16 groups (384 channels maximum), or 16 single channel inputs at either 16 or 32 Kb/s.
TRI-TAC Subchannels	16 full duplex ports on 2 boards. Allows 16 each of 2 or 4Kb/s subchannel inputs and supports reassignment of up to 48 subchannels.
T1 to TRI-TAC Conversion	2 modules. Allows conversion of up to 82 T1 channels to TRI-TAC and up to 192 TRI-TAC channels to T1.
Automatic Sparing of:	RAN SCRAN Recirculator Timing Power Supplies

Computer monitoring and display of performance of all modules.

The CRM is modularly expandable. A single card frame can be used to interface up to 40 ports. The address space and wiring in the CRM support one to seven card frames. Each of these frames may be populated with any types of interface cards desired.

The CRM is made fault tolerant by the inclusion of spare circuit cards for critical functions. When certain faults are indicated in the

built-in test data generated in the CRM hardware, the CRM software automatically switches to one of the spare circuit cards. A message indicating that this action has been taken is displayed by a CRT connected to the CRM and sent to the Network Control computer.

The built-in test data includes framing and activity indicators on incoming bit streams. Thus, this data serves as an indicator of the status of the transmission links connected to the CRM. This supports fault isolation and performance assessment by the CRM directly.

The Network Control System

The Transmission Network Control system in the DCS is required to maintain the circuit paths in the DCS. It performs this task by monitoring the transmission system status and finding alternate routes (i.e., "altroutes") for circuits in the event of failures in the transmission system. The required Network Control operations in the event of a system failure are as follows:

1. Detect transmission outages (links, groups or channels).
2. Identify the circuits effected by maintaining records (in real-time) for circuit, route and status data.
3. Attempt to generate altroutes for high priority users.
4. Maintain a control telemetry network.

The automation of these Network Control tasks is facilitated through a network-wide deployment of CRMs at DCS stations and the installation of primary and back-up Network Control sites. These sites together with an adaptive packet telemetry system make up the proposed automation of Network Control. We will now examine the required Network Control tasks mentioned above in detail and discuss their automation.

Detection of transmission system faults is the first step towards service restoral via altrouting. There are two sources of such data: ATEC and CRMs. ATEC can provide detailed hardware fault identification which in turn identifies functional link/group/channel outages. The CRM too can provide this functional information. Since it monitors group activity and framing, it can detect most types of failure directly. By using the CRM's remote controlled patching capability, test bit streams can be inserted and traced to detect more subtle faults (Figure 4). Since the CRMs are already in contact with Network Control to receive patching commands, a robust telemetry network is already present to send faults from CRMs to the Network Control site. Note that CRMs do not sense the equipment that may have failed but only the functional result of the failure. This is all that is required, however, for Network Control's mission. The altroute can be implemented without specific knowledge of the equipment failure mode.

A final interesting point concerning fault detection is the issue of circuit-level failures in a network with CRMs at every station. In such a network, channels appear by themselves only at the user loop (which is outside of the transmission system) or within the CRM itself. Since Network Control does not directly address user loop faults, all transmission system channel faults are directly accessible by the CRM for detection.

Once the faults in the network have been determined, it is the job of the Network Controller to determine the functional circuits affected. The proposed system uses a versatile network-type data base (Figure 5) with a full data base management system (DBMS) to facilitate this step. Both permanent and temporary circuit records are kept. These records are linked chains of appropriate link, group, station, channel and fault status records. New fault status data is constantly entered into these records. These new

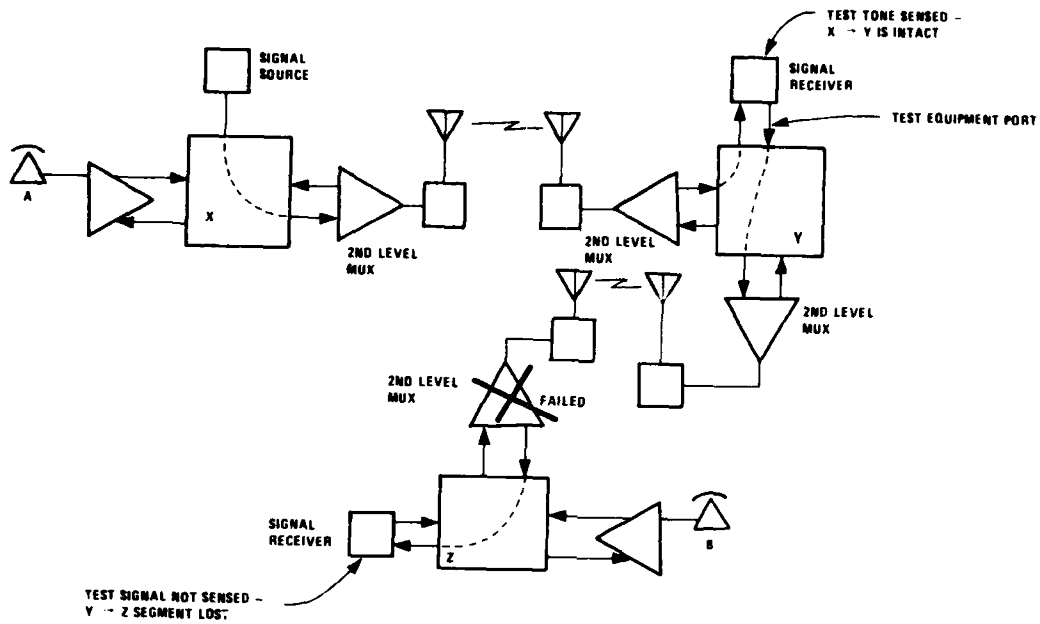


Figure 4. CRM Fault Isolation via Signal Trace

entries also prompt status display changes and altrouting task queueing.

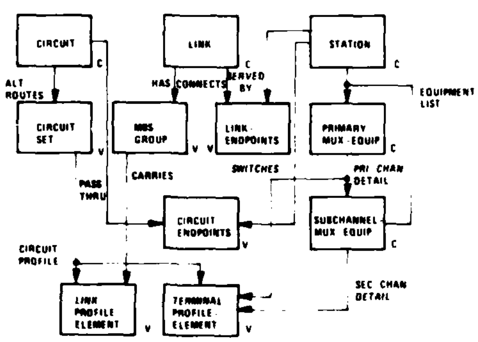


Figure 5. Network Control Data Base Schema

The next step in the Network Control tasks is the establishment of alternate routes for high priority users. We have proposed a dual approach to this task. A set of route building displays has been developed to easily guide an operator through a manual altrouting process. In addition, an automatic route building algorithm has been proposed for service restoral in a minimum of time. These two tools are integrated into a single algorithm which provides maximum versatility for the route selection task. The operator is afforded the opportunity to examine the altrouting queue and select the degree of personal interaction at every step along the way. The automated route building algorithms provide generation of a number of optimum routes under the control of operator metrics and weighting factors.

In addition to patching automation, the altrouting opportunities available to the operator (or the automated routines) are also enhanced by the presence of the CRMs. A CRM at every DCS station allows circuit route patching at every station. This is currently not possible in the DCS because circuit patching requires first level multiplexers (Figure 6) and not every group

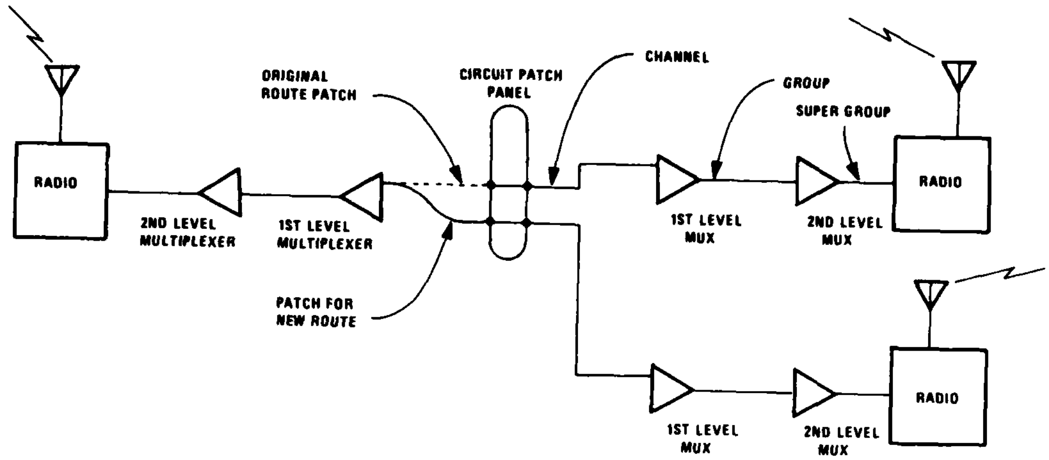


Figure 6. Current Channel Patching

brought into a DCS station is broken down to this level. With the CRM at a station, the multiplexers used for circuit routing are eliminated and every circuit entering the station has route patching capability (Figure 2). The connectivity of the network is, thus, enhanced by CRM deployment.

To protect the Network Control system from hardware failures or network changes, the system must be made adaptively reconfigurable. The system must have primary and back-up control sites in the event a control site is not operational or the network becomes split into subnetworks due to link or station outages. There must also be a means for determining new control site responsibility in the event the network divides along any arbitrary lines. In addition to redundant control sites, the telemetry system (which uses DCS links as well) must be made flexible enough to adapt to back-up control site relocation and a changing network reconfiguration. The most effective method for meeting these redundancy requirements utilizes telemetry routing algorithms which are adaptive apriori of any set of expected failure scenarios.

The Network Control system under current contract at Honeywell is the first step in a validation of the automated controls discussed above. The validation system will be hosted on a PDP-11/34 computer and interface both real and simulated CRMs in a 13-node network. The validation system will handle fault reports from a simulation fault generator which is controlled by a simulation terminal on the 11/34. Both operator-assisted and fully automated altrouting will be provided. In addition, there will be alphanumeric and graphic operator interfaces made available.

The current validation Network Control program will provide an important first step in automated transmission Network Control for the DCS. As such, it can be used for evaluation of CRMs, controlling DEB test bed experiments, and tech controller operator training. Successful validation will lead to incorporating the multiple control sites and adaptive telemetry necessary for completion of the full concept validation.

The work described in this paper was supported by Rome Air Development Center and the Defense Communications Engineering Center.

REFERENCES

1. Digital Network Control and Concept Development, Phase I Final Report, Contract DCA100-79-C-0030, December 1979.

2. Design Plan, Channel Reconfiguration Feasibility Model, Contract F30602-79-C-0052, June 1979.

3. System Control for the Transitional DCS, Reports 3 and 4, Contract DCA100-78-C-0017, July 1979.

BIOGRAPHIES

Mr. Arnold A. Argenzia is a Project Engineer in the Communications Control Division of Rome Air Development Center. Since 1974, he has been involved in improvements to the Technical Control and System Control for the Defense Communications System.

Mr. Argenzia was previously involved in Line of Sight and Tropospheric communications and coding theory.

He received his Bachelor's degree in mathematics from Syracuse University.

Ronald K. Crowe is the Section Chief for Communications Technology. In this position, he has the final technical and financial responsibility for all programs executed by or for the Communications Technology Section. Current contracts are the Channel Reconfiguration Feasibility Model (CRM) and Digital Network Control and Concept Development.

Mr. Crowe previously was the project engineer and lead system engineer on the Channel Reconfiguration Feasibility Model contract with RADC. Mr. Crowe also contributed to technical aspects of the Digital Network Control contract.

On previous assignments, Mr. Crowe was the lead engineer for the contract System Control for the Transitional DCS. On an internally funded program, he was responsible for requirements definition and conceptual design of equipment performing the digital channel reassignment function. He has analyzed the DCS operation and configuration, including the AUTOVON and AUTODIN systems and the terrestrial and satellite transmission plant.

Ben E. Simmons is a Senior Principal Research Scientist in the Communications Technology section of Honeywell's Systems and Research Center. Mr. Simmons is currently project engineer on the Channel Reconfiguration Model program.

Prior to joining SRC, Mr. Simmons was a member of the Advanced Development group at Honeywell's Avionics Division in St. Petersburg, Florida. Here he participated in the design and development of the AN/USC-26 Group Data Modem. Mr. Simmons also designed a series of CVSD voice digitizers, including a hybrid microcircuit version and a CVSD channel bank.

Robert V. Krzyzanowski is a Senior Research Scientist at Honeywell's Systems and Research Center. He is a member of the Communications Technology section where he contributes expertise in the telecommunications transmission, system analysis and analog circuit design.

Mr. Krzyzanowski has contributed to the Network Control program at Honeywell in the areas of routing algorithms and control techniques. While with Honeywell, he has also worked in fiber optics communications, radar receivers and mobile radio interfacing.

Prior to joining Honeywell, Mr. Krzyzanowski worked as a designer with the North Electric Col. and later with the Vidar Division of TRW. With the North Electric Co. he designed hardware for subscriber signalling and transmission as part of a digital telephone switch development. At Vidar, he designed transmission equipment for digital wire systems and performed analysis in bandwidth compression and clock recovery for such systems.

TEST SYSTEMS FOR BASE/ACCESS AREA CRITICAL USER OPERATIONAL READINESS*

John F. Sawyer
The MITRE Corporation
McLean, Virginia

Purpose

The purpose of this effort is to assure that critical DCS user circuits have a high level of operational readiness. This study focuses on the DCS user's access lines and dedicated circuits between users.

A major objective is to assess the ATEC system's potential for monitoring and assessing communications performance in the base/access area. Alternatively, for areas where the ATEC is not deployed, it is also important to evaluate non-ATEC means of monitoring, transmitting, and processing base/access area performance information. This paper compares the relative costs and benefits of a number of candidate test system alternatives which comprise both ATEC and commercially available test elements.

Test System Roles

Figure 1 shows the relationship of base/access area testing to critical DCS user circuit operational readiness. Three levels of testing are considered:

1. Catastrophic end-to-end failure tests
2. Fault isolation tests
3. System degradation tests.

---

* Review of this material does not imply Department of Defense endorsement of factual accuracy or opinion.

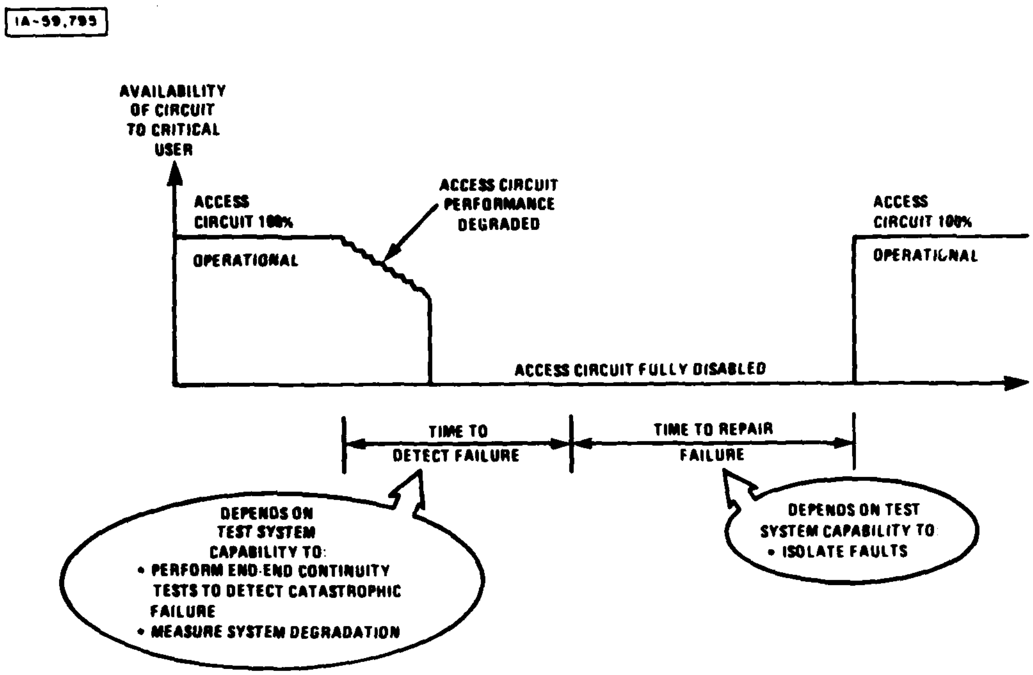


Figure 1. RELATIONSHIP OF BASE/ACCESS AREA TESTING TO CRITICAL USER CIRCUIT OPERATIONAL READINESS

Currently critical circuit failures are detected when the user attempts to use the communications system and discovers it is disabled. Frequent end-to-end continuity tests of critical circuits would detect catastrophic failures with reduced average failure detection time and improve the operational readiness percentage of these circuits. With typical repair times on the order of one-to-two hours, end-to-end continuity tests should be performed at a minimum, at least several times per hour (even continuously), to assure prompt detection of catastrophic failures. These end-to-end continuity tests are the single most important tests to assure operational readiness of the critical user circuits.

Given prompt detection of catastrophic failures, the second most important type of tests are those designed for fault isolation. Good fault isolation testing can rapidly pinpoint the failure, save jurisdictional discussion, and reduce the repair time. Hence, both end-to-end continuity testing and fault isolation testing are extremely important to improved operational readiness of critical user circuits.

The third type of testing, system degradation testing, addresses the more nebulous worlds of "fine tuning" and "failure prediction". This type of testing can provide higher quality average communications service to the user. It has the potential of averting at least some catastrophic failures if the testing is well implemented and preventive maintenance is performed. Because the payoff of system degradation testing is less clear-cut, this type of testing is the least important of the three types considered for operational readiness enhancement and should be implemented only in specific cases where definable advantages can be realized at modest incremental cost.

Analysis Approach

The overall approach to the study was to (1) identify the number of critical circuits in the European theater requiring base/access area monitoring, (2) define the alternative test system arrangements that should be considered for this purpose, (3) obtain cost data for the test components, (4) weigh the system factors in terms of importance and (5) derive the cost/benefit score of each alternative test system. Additionally, deployment of the test systems in the European theater and potential extension of their capabilities to the European Telephone System (ETS) are also briefly addressed. The test system arrangements examined all have the same basic elements (1) a central information collection/processing facility, (2) sensors and probes to collect quality monitoring and fault isolation information, and (3) a means of transmitting that information from remote terminal stations to the central processor located at the ATEC node.

Table 1 identifies the twenty-three test system arrangements considered and their suitability to the prime mission of catastrophic end-to-end failure detection and fault isolation testing. Only six systems thoroughly meet the primary test objectives; ten others also represent a partial solution to the test problem. The arrangements were developed to make maximum use of existing signals, alarms, and range from the simplest (low cost) to the very comprehensive (high cost and interface complexity).

To assess the number of circuits to be monitored for the DCS in Europe, subsets of critical DCS circuits were examined based on Restoration Priority (RP) and Maximum Calling Precedence (MCP). The analysis derived the number of circuits in each subset.

There are 7265 circuits to be considered in the European theater including access lines and dedicated circuits. Depending on the critical subset selected, between 30 and 2332 of these will be the prime candidates for base/access area monitoring.

Although the overall study focuses on the entire DCS in Europe, it was felt important to examine in more detail how the test system might be applied in a specific area. An approximation to an actual ATEC nodal subnetwork - the Linderhof Nodal Subnetwork - was analyzed. This complex was selected because it is rich in the "analog endlink" appended to "digital backbone" configuration typical of the analog-to-digital transition period of the middle-to-late 1980's. The analysis concentrates on the analog endlink connecting the ATEC station to the terminal Technical Control Facility or station from which the user is served. Cost and benefit weightings were assigned to each arrangement based on an interpretation of the Linderhof Nodal Subnetwork that most closely resembles planned ATEC deployments.

The set of desirable arrangements obtained from this analysis of the Linderhof Nodal Subnetwork is virtually the same as that arising from the analysis of the RP and MCP subsets of the DCS throughout Europe.

Conclusions

Table 2 shows the four preferred test system arrangement evaluation scores. There are three ATEC-based choices (economy through deluxe) and one non-ATEC based choice. Arrangement 12, consisting of an ATEC ARS and IMS augmented with a Circuit Continuity Tone Injection/Detection and Noise Measuring (CTIDN) device is a reasonable all-round choice (cost vs. capability) because of its ability to do full-time catastrophic end-to-end failure detection of critical circuits and to measure all critical circuit parameters on both an automatic or a "monitor immediate" basis.

Although Arrangement 12 monitors most of the transmission system and facilities in the base/access area, it does not test the final loop to the user handset. Arrangement 18 (Deluxe ATEC), expands upon Arrangement 12 to include a Loop Reporting System (LRS) that additionally measures the end-to-end continuity to the user handset. If the fault location statistics generated during the testbed phase of the base/access area test system implementation program demonstrate that inclusion of the LRS is warranted, the basic Arrangement 12 can be expanded to the Deluxe ATEC Arrangement 18, recognizing added investment dollars will be needed as shown in Figure 2.

Costs of implementation vary with the number of circuits to be monitored. Figure 2 shows the initial investment costs of the four preferred test system arrangements as a function of the number of circuits covered. System life cycle costs are generally proportional to the initial investment cost.

TABLE 1

TEST SYSTEM ARRANGEMENTS CONSIDERED AND THEIR SUITABILITY TO THE PRIME MISSION

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
ARS MONITORS MUX PILOT ALARM	x	x	x			x	x	x	x	x	x	x	x			x	x	x	x				
ARS MONITORS E&M LEADS OF SF		x																					
ARS MONITORS DFSU ALARM LEADS			x					x		x							x						
ARS MONITORS CTIDN* ALARM LEADS											x	x	x					x	x				
DATALOCK MONITORS MUX PILOT ALARMS														x	x								
DATALOCK MONITORS DFSU ALARM LEADS														x									
DATALOCK MONITORS CTIDN ALARM LEADS															x								
IMS MONITORS VOICE CIRCUIT PARAMETERS				x	x	x	x	x	x	x		x	x			x	x	x	x				
IMS MONITORS SF TONE CONTINUITY					x		x		x							x							
PCS MONITORS ANALOG RADIO LINKS									x	x			x			x	x		x				
LOOP REPORTING SYSTEM																x	x	x	x			x	x
H.P. SIMPLE AUTO. TEST SYSTEM																				x		x	
H.P. MODERATE AUTO. TEST SYSTEM																					x		x
PERFORMS THOROUGH CATASTROPHIC, END-TO-END FAILURE AND FAULT ISOLATION TESTING	NO	LESS THAN FULL TIME	LESS THAN FULL TIME	NO	LESS THAN FULL TIME	NO	LESS THAN FULL TIME	LESS THAN FULL TIME	LESS THAN FULL TIME	LESS THAN FULL TIME	YES	YES	YES	LESS THAN FULL TIME	YES	LESS THAN FULL TIME	LESS THAN FULL TIME	YES	YES	NO	NO	NO	NO

*CTIDN = Circuit Continuity Tone Injection/Detection and Noise Measuring

TABLE 2

RECOMMENDED TEST SYSTEM ALTERNATIVES

ARRANGEMENT NUMBER	SELECTION BASIS	TEST BENEFIT SCORE (700)	COST SCORE (300)	COST/BENEFIT SCORE (1000)
11	LOW-COST ATEC CHOICE	514	264-298	778-812
12	BEST ALL-ROUND ATEC CHOICE	530	246-278	776-808
15	BEST NON-ATEC CHOICE	479	270-299	749-778
18	DELUXE ATEC CHOICE	580	190-246	780-826

It is concluded that there are test techniques currently commercially available or well within the state of the art for the base/access area monitoring of critical DCS users and that the recommended arrangement(s) should be implemented immediately. A follow-on study to examine the applicability to the new ETS design is also timely and needed.

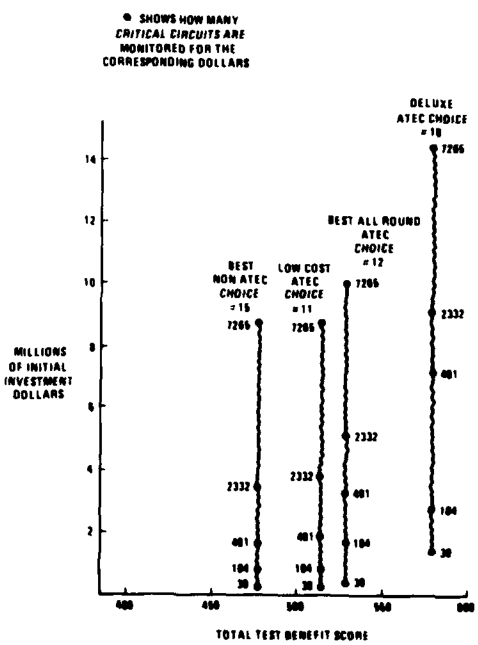


Figure 2 COST BENEFIT SUMMARY OF PREFERRED TEST SYSTEMS

MANAGEMENT OF DATA FOR CONTROL OF A MILITARY COMMUNICATION SYSTEM

B.J. Leon
University of Kentucky
Lexington, Kentucky

Capt. J.R. Monastra, USA
United States Military Academy
West Point, New York

D. Spector
Rome Air Development Center
Griffiss Air Force Base, New York

ABSTRACT: Control of a communication system requires considerable data. Proper management of these data is essential. This paper discusses the data required for control and shows that the data fit into four distinct bases. Each data base has different properties that require different file structures for management. A discussion of the data bases and appropriate structures therefore are presented.

BASIC CONCEPTS

For a general purpose, multi-user, telecommunication system, effective control requires information from four data bases. The first of these is information about the users. Who are they; where are they; how do they communicate? The second base of data is a description of the installed communication system as it was designed. The third base of data contains information on the current condition of the communication assets. The fourth contains the information on current and projected usage. Before elaborating further on the data and how it would be managed for effective system control, let us define what we mean by system control.

<u>Telecommunication system control is the control of access to communication assets in order to maximize a performance measure established by management</u>. Access by both users and maintenance personnel must be controlled. The performance measure assigns values to the various classes of messages and the time required to initiate, transmit, and receive these messages.

In a military communication system there are many different types of messages submitted by many different users. Voice messages are submitted for either clear or se-

cure transmission. Data messages of many types are submitted. Standard text traffic, facsimile data, computer file transfers, intelligence data, brief fire control messages, etc., are all contained as classes of data. Video is not now a major part of military communication, but it may well be in the future. The timely delivery of each message varies in importance depending on the type of message, the particular individuals (including equipments) sending and receiving the message, and the military situation. The military commanders must quantify the significance of the various messages under the various defense readiness postures. This quantification is the "management set performance measure". The perfect communication system delivers every message in a timely manner. Since we can't afford the perfect system, we must design a control to assure that the most important messages get through first. The description of the users, the messages they may submit, and the significance value associated with each message is the data for base one. We shall call these data the generalized phone book.

The communication assets potentially available to meet Command and Control requirements are a diverse collection of specific systems designed and installed piecemeal to meet specialized needs. In the present command structure assets are often separated into strategic and tactical categories. Often the procedures by which the assets for each category are selected are different. Furthermore, new special and general purpose circuits are constantly in various stages of development. A total catalog of these assets--where they are, how they work, how access is obtained, etc.--is data base two.

Much of the recent efforts in system control are extensions of technical control. Most of the subsystems of the total communications system were laid out with specific locations where technical controllers are placed to regularly test the performance of the network components to see that they are operating up to the design specifications. When components are out of spec, tech control is responsible for scheduling maintenance and restoration. The information gathered by tech control, whether manually gathered or automated through a system like ATEC, makes up data base three. The scheduling of maintenance and restoral is the control of access of maintenance personnel. Thus system control includes tech control.

The real key to effective system control is the adaptation of the access to the system assets to meet varying levels of user demands. At the present time, except for a few manual procedures, the only parts of the system that are controlled by demand are the switched AUTOVON, AUTODIN, and AUTOSEVOCOM. The presently planned Tri-Tac system will bring such sharing to the tactical arena. If better traffic data were available on a near real time basis, circuits could be shared between systems to give better satisfaction of user needs. At present in Europe when AUTOVON is heavily overloaded, there are unused circuits in the DCS that parallel the AUTOVON trunks. Better use data would allow system control to give the important voice users access to these now unused circuits. Data base four is the traffic data that is not now available for real time system control.

To summarize:

Data Base One -- The generalized phone book including user precedence levels.

Data Base Two -- The physical system architecture as designed and installed.

Data Base Three -- The serviceability of the various assets -- in service and in spec, in service but degraded, or out of service, along with the reason for outages.

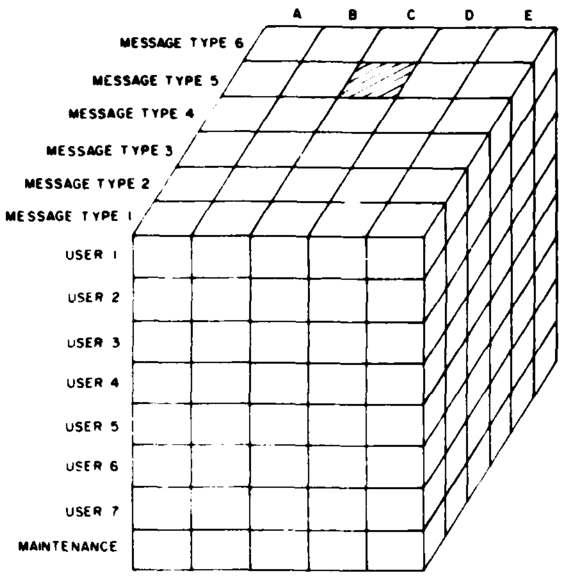
Data Base Four -- System traffic and service demands.

THE NATURE OF THE DATA BASES

The structuring of a data base depends on how the data must be accessed and how frequently the data changes. <u>Let us examine the four data bases to see which significant properties apply</u>.

Since Data Base one is a generalized "phone book", frequent additions and deletions on a real time basis would not be anticipated. Thus, since data base one is a "static" file which will need fast random access, the sequentially allocated linear list data structure was chosen. It allows for fast random access with a minimum of overhead while providing acceptable insertion and deletion time for changing the "static" file of data base one when needed. Figure 1 is the architecture of data base one.

PRECEDENCE LEVEL



NETWORK PRIORITY MATRIX
Figure 1

Since Data Base two is to reflect how the network is interconnected and since real time changes are not anticipated, data base two is a "static" file. Thus a linked linear list data structure was chosen because fast sequential processing will minimize the routing selection speed. An example of the data base structure for a four node network is shown in Figure 2.

Figure 2

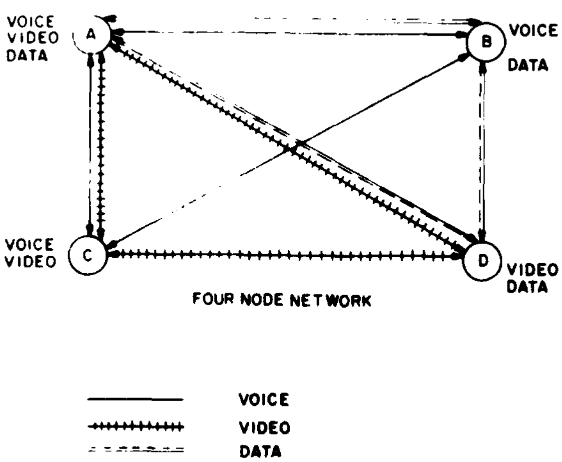


FIGURE 2 (CONTINUED)

NODE ID	VOICE LINK	CHANNEL FIELD	LINK	VIDEO LINK	CHANNEL FIELD	LINK	DATA LINK	CHANNEL FIELD	LINK
A	C	xxxx	B	D	xxxx	C	D	xxxx	B

STRUCTURE NODE A

NODE ID	VOICE LINK	CHANNEL FIELD	LINK	VIDEO LINK	CHANNEL FIELD	LINK	DATA LINK	CHANNEL FIELD	LINK
B	A	xxxx	C	0	0000	0	A	xxxx	D

STRUCTURE NODE B

NODE ID	VOICE LINK	CHANNEL FIELD	LINK	VIDEO LINK	CHANNEL FIELD	LINK	DATA LINK	CHANNEL FIELD	LINK
C	B	xxxx	A	A	xxxx	D	0	0000	0

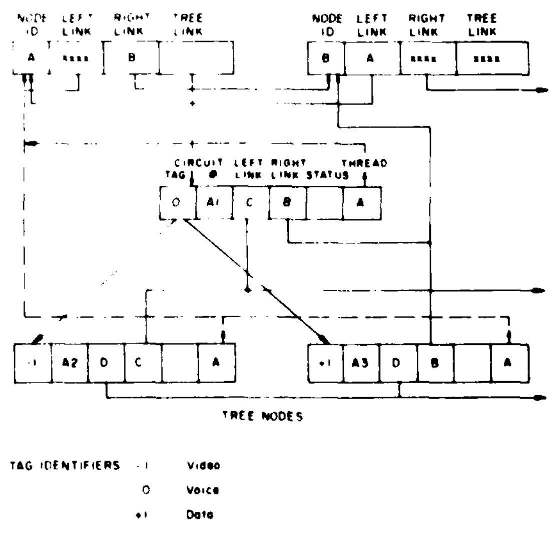
STRUCTURE NODE C

NODE ID	VOICE LINK	CHANNEL FIELD	LINK	VIDEO LINK	CHANNEL FIELD	LINK	DATA LINK	CHANNEL FIELD	LINK
D	0	0000	0	C	xxxx	A	C	xxxx	A

STRUCTURE NODE D

Since Data Base three is an up to date serviceability report of the network links, it will have frequent real time changes. Since data base three is a "dynamic" file, a linked linear list with a binary status indication tree was selected in order to have fast insertion/deletion time as well as fast sequential processing time to reduce routing speed. The example of the hybrid link linear list with a binary status tree is shown in Figure 3.

Figure 3
MAIN LIST NODES



NOTE: Link fields are filled in accordance with the simple four node circuit used as an example throughout this paper

Since Data Base four is an up to data "picture" of traffic and a prediction of future traffic based on a historical analysis of past traffic, it will have frequent real time changes. Thus, data base four is a "dynamic" file. A binary tree file structure was chosen so as to provide for the capability of being "copied" and analyzed quickly. The size of data base four will be determined by management criteria as to how much projected data is needed.

DATA BASE USAGE

An example of the generalized "phone book' which is data base one is depicted in Figure 1. Data base one is a three dimensional priority matrix within which resides the Network User Priorities (NUP) of each user for different messages and different military situations. In order to determine an NUP for a requesting user, the system searches for the user, message type, and precedence level to locate the cell of the priority matrix where the NUP is stored. For example, suppose that user 1 has requested service in order to send a message type 5 of precedence level C. The system would determine the NUP for the request to be that stored in the hatched cell of Figure 1.

A four node network example of the physical system architecture which is data base 2 is depicted in Figure 2. The structure node A in Figure 2 describes all of the existing circuits and circuit types which are connected to node A, and which nodes are connected to node A. The first block of the structure node indicates which node the structure node is describing -- in this example it is node A. The next three blocks of the structure describe possible voice circuit links -- in this case a voice link to nodes C and B. The channel field contains information about the voice circuits -- such as circuit numbers. The next three blocks of the structure describe the possible video links in the same manner as the previous voice links. The last three blocks of the structure describe the possible data links in the same manner as the previous voice link blocks. Note that in this simple example that the voice, video, and data links can each have a maximum of two links; whereas, in a "real" system the maximum number of links will be set either by management criteria or by the existing physical system architecture at the time of the system implementation.

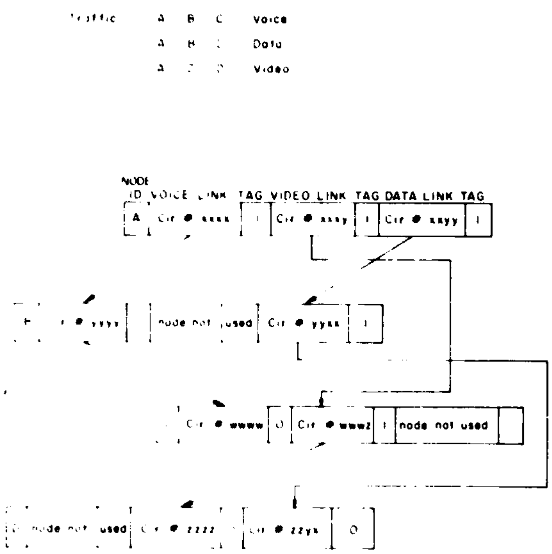
The serviceability information for a portion of data base 3 designed to describe the simple four node network of Figure 2 is depicted in Figure 3. Examining the main list node for node A in Figure 3, the first block indicates which node is being described. The second block indicates which node is linked to the described node from the left (left link); whereas, the third block describes the node which is to the right (right link). The last block is the three link which refers to a specific status indication tree for the circuits which pass through this main list node. The status indication tree is a binary tree composed of three "branches" each of which contains a description of a circuit for a specific message type. The message types are indicated by the tag identifiers (in this example -1 is video, 0 is voice, and +1 is data).

A "branch" structure of a status indication tree contains a block which indicates the message type by a tag identifier, a block with the circuit number, a block indicating the node on the circuit which is considered to be connected to the main list node from the left (left link), a block indicating the right link, a block indicating the status or serviceability of the node, and a block called the thread which indicates how to relocate the main list node that is being described. This data base would be utilized by a node by node check of the serviceability of the desired route by: locating the requesting users node, locating the appropriate status indication tree branch through the utilization of the tree link and tag identifier, checking the serviceability of the circuit by the utilization of the status block and going to the next main list node in the route. For example, suppose a voice message is to be sent from node A to node B. The system would start at the node A main list, locate the status indication "branch" desired by utilization of the tree link block and tag identifier, check the serviceability of the circuit by utilizing the status block, and use the right link block to reach main list node B. Note that in this example only one status tree branch needed to be examined. If a message were to be routed through several nodes, several status tree branches would be examined.

An example of the "traffic" usage of data base 4 is depicted in Figure 4 with the tag fields as previously described. Data base 4 can be copied at certain time intervals and historically analyzed in order to produce projected traffic for the future. In other words, the "traffic" data can be

Figure 4

The following traffic is generated as an example to illustrate the field contents of each node. It should be noted that the circuit number will automatically establish the next node relationship of the tree



copied every 15 minutes and compiled to produce hourly projected traffic, the hourly traffic compiled to produce daily projected traffic, the daily traffic compiled to produce weekly projected traffic, etc.

GEOGRAPHIC CONSIDERATIONS

The system control operations described herein can be carried out either from a single central location or from theater control centers that are dispersed throughout the overall communication system. The latter arrangement is certainly preferable from the point of view of survivability of a military network. In the distributed control arrangement one must be sure that serviceability data for each circuit is given to all control centers that may dedicate that circuit to use so that data base three is up to date at each center. We must also be sure that when a particular center does dedicate a circuit, the usage updates are sent to the other appropriate control centers that may also consider using that circuit.

With distributed control, the various data bases need not be stored in their entirety at any of the local control center. Only local data and interconnection data need be kept at each location. This gives better immunity to enemy intelligence operations.

SPECIFIC SYSTEMS AND RELATION TO THE TOTAL SYSTEM

At present only AUTOVON, AUTODIN, and AUTOSEVOCOM have any automated control. AUTODIN can use AUTOVON trunks with modems. This is the only intersystem usage except for manual restoration priorities that allow controllers to manually reassign transmission trunks. As new systems are added to the total set of communication assets, some though should be given as to how any new system can share assets with old systems. With digital transmission, such as is now being installed in the Digital European Backbone, the ability to efficiently interchange data at various speeds with both clear and secure voice is possible. The multiplexers and their controls can handle the problem if good system control is instituted. The propopsed TRI-TAC equipment is also compatible with the DEB. Proposals have also been made to integrate packet and message switching. Thus overall system control should be planned.

CONCLUSIONS

In this paper the basic data structures for system control have been discussed with only passing reference to specific problems. The concept of overall system control seems feasible. The next step is to get specific data base sizing.

The starting point should be data base 2. Communications assets are specific, but it is difficult if not impossible to find a catalog of the assets as they stand today. Thus the first step is to develop such a catalog in a unified format. Present equipment should be documented first. Then all outstanding procurements with projected service dates should be integrated into the catalog.

Next data base one can be constructed. From the listing of assets the listing of users can be developed. As this listing evolves it can be turned over to the General Staff so that the priorities can be set.

The procedure for obtaining data base three must be established by examining base 2. An examination of each system in the field should show the provisions currently available for monitoring circuit service-

ability. As ATEC evolves, it can be integrated into the data gathering process for data base 3.

The gathering and use of traffic data is still not well understood. The area where research can bring large payoffs is the use of these data in overall system control. However, traffic cannot be studied in isolation. We can begin to capitalize on the use of traffic data only when the use of the other three data bases is understood.

BIOGRAPHY

Benjamin J. Leon received the B.S. degree from the University of Texas (1954), the S.M. degree (1957) and Sc.D. degree (1959) from the Massachusetts Institute of Technology.

He joined the University of Kentucky as Professor and Chairman, Department of Electrical Engineering in 1980. Prior to joining UK, he was on the faculty of Purdue University from 1962 until 1980. During his sabbatical years, he was Visiting Professor at Cornell University (1968-59), Electronics Engineer at the Defense Communications Engineering Center (1975-76) and Consultant for Westinghouse (1980). Prior to his affiliation with Purdue University, he was on the staff of Lincoln Laboratories (M.I.T.) and Hughes Research Laboratories. He has consulted with Components Corporation ARINC, Akron Brass and the Bell Telephone Merrimack Valley Laboratories. From 1964-73 he was the Consulting Editor for the Holt, Rinehart and Winston, Inc.

In addition to supervising graduate thesis work at the M.S. and Ph.D. level, Dr. Leon has published some three dozen papers, two books, and several book chapters. He holds a U.S. patent. For 1979 and 1980, Dr. Leon is the Vice-President Educational Acitivites of the IEEE. He is a past editor (1967-69) of the IEEE Transactions on Circuit Theory and past chairman of the Circuit Theory Group of the IEEE. He has also held numerous positions with the Standards Board and the Central Indiana Section of IEEE. He is a Fellow of the IEEE and a member of AAAS, AAUP, Tau Beta P, Eta Kappa Nu, Sigma Xi, and Phi Eta Sigma.

PANELS

Panel One: Performance Assessment and Methods for Controlling Integrated Systems

Chairperson: Spurgeon Watford
Ford Aerospace and Communications Corporation
Colorado Springs, Colorado

Biography:

Spurgeon E. Watford is currently responsible for key elements in the system design and analysis for ATEC program at Ford Aerospace and Communications Corporation. Before his association with FACC Mr. Watford was a group leader with the MITRE Corporation. He has been involved in the analysis, design and implementation of communications transmission, switching, monitoring and control systems for 20 years. He has exercised key engineering roles in the NORAD Cheyenne Mountain Complex Project, the SAFEGUARD program, AUTODIN and AUTOVON.

Mr. Watford received a Bachelor of Science degree in Electrical Engineering from New Mexico State University.

Members:

P. Jeffrey Bogert
Stanford Telecommunication, Inc.
Palo Alto, CA

John Conley
Ford Aerospace and Communications Corporation
Colorado Springs, CO

Warren Hawrylko
Defense Communications Engineering Center
Reston, VA

Dennis Hicks
AT&T Long Lines
Washington, DC

Panel Two: Implications of System Control on Survivability

Chairperson: Thomas Yium
Air Force Communications Command
Scott AFB, Illinois

Biography:

Mr. Thomas Yium is Director of Studies and Analysis for the Air Force Communications Command (AFCC), Scott AFB, ILL. The Command's mission includes engineering, installing, operating and maintaining communications-electronics and meteorological facilities for all Air Force commands, and selected government and civilian agencies. These responsibilities encompass long haul inter-continental and local base communications, automated data processing systems, air traffic control, and navigational aid facilities and services.

Mr. Yium received a bachelor of science degree in aeronautical engineering in 1955 and a master of science degree in mechanical engineering in 1956 from the University of Texas, and a master of science degree in electrical engineering from the University of New Mexico in 1964.

Mr. Yium was commissioned a second lieutenant in the U.S. Air Force in 1955, serving as a design engineer with the Special Weapons Center, Kirtland AFB, N.M. until 1959. Upon discharge, he accepted a Civil Service position with the Test Directorate at the same command.

Later positions include: electronics engineer, Air Force Weapons Laboratory, Kirtland AFB, N.M.; and operations research analyst, Joints Test Force 2, Sandia Base, N.M., in the Directorate of Analysis and Reports.

In 1969, Mr. Yium accepted a position in AFCC in the Operations Research Analysis Office and was subsequently selected as Director in 1975. As senior technical advisor to the Commander of the Air Force

Communications Command, he plays a key role in formulation of technical policy and the development of scientific methodology for solving operation and communication-electronics maintenance problems. He has conducted studies or established programs related to power systems, survivability, weather and ionospheric effects on communications and navigational aids, digital data network maintenance and management as well as other mission-related areas.

Members:

Alan D. Campen
BDM Corp.
McLean, VA

Robert L. Feik
Consultant
Annapolis, MD

Col. Bobby Smith, USAF
Commander, DCA-European Area
Stuttgart, F.R.G.

Panel Three: Operational Aspects of System Control

Chairperson: Colonel Clifford O.C. Henning, Jr.
Air Force Communications Command
Scott AFB, Illinois

Biography:

Colonel Clifford O. C. Henning, Jr. is the Assistant Deputy Chief of Staff, Operations, Plans and Readiness, HQ Air Force Communications Command, Scott AFB, Illinois.

Colonel Henning served as a maintenance officer on the first "blue suit" maintenance team of the Semi Automatic Ground Environment (SAGE) computer system. He was also assigned to the Ballistic Missile Early Warning System (BMEWS), first as a computer maintenance officer at the contractor project headquarters and then as a ground electronics officer at BMEWS Site III in England.

Later, he served at the Defense Communications Agency, Washington D.C., as the chief of the Transmission Facilities Management Division of the Operations Directorate. Colonel Henning assumed duties as Assistant Deputy Chief of Staff, Communications-Electronics for Headquarters, U.S. Air Forces in Europe in August, 1976. In May 1978, he was named Commander of Defense Communications Agency, European Area, and then in July 1980 he assumed his present position.

Colonel Henning received a bachelor of science degree from Oregon State University and a master of science degree in business administration from George Washington University. He was a distinguished graduate of the Air Command and Staff College in 1967, the Industrial College of the Armed Forces in 1970, and graduated from the National War College in 1972.

Members:

Major (P) John B. Class
Hq., U.S. Army Communications Command
Ft. Huachuca, Arizona

Col. William J. Dobson, Jr.
Defense Communications Agency
Arlington, VA

Capt. John J. Flynn, USN
Naval Telecommunications Command
Washington, DC

Larkin B. Vance
Hq., SHAPE
Mons, Belgium

DEMONSTRATIONS

MITRE COMMUNICATIONS NETWORK ROUTER

H.A. Neimeier & R.J. Portal
The MITRE Corporation
McLean, Virginia

Router Definition

A Router is a software implementation of a mathematical algorithm for finding the shortest path (minimum metric) between selected node pairs on a specified communications network.

Router Uses

The microprocessor-based interactive router program described here can perform the following functions on large networks (500 nodes and 2000 links):

- Channelize a network (assign user communications requirements to a transmission system)
- Identify which requirements are interrupted by loss of any number of communication facilities
- Suggest alternate paths for the above interrupted requirements. (This permits real-time restoral of disabled circuits
- Provide path survivability estimates over a broad range of conflict scenarios
- Evaluate the survivability and efficiency of alternate network topologies
- Quantitatively evaluate the benefits of (1) flexible multiplex equipment, (2) an adaptive satellite policy, or (3) internetting with other networks
- Calculate the needed transmission link capacity so that all requirements can be routed via their minimum metric path

- List lease requirements that should traverse military transmission and military requirements that should be leased.

- List nodes in order of their criticality and perform network stress analysis studies.

The Channelization Process

The channelization process allocates transmission facilities to satisfy communication requirements. Circuit routes can be automatically determined which meet such objectives as:

- Minimum length
- Maximum survival probability
- Path and media diversity
- Location avoidance
- Minimum cost
- Maximum transmission quality.

Further, the MITRE router algorithm employs metrics to optimize weighted combinations of the above objectives. To do this a number (or metric) is assigned to each transmission link based on its characteristics such as:

- Length
- Survival probability
- Medium Type
- Cost
- Transmission quality.

This list of communication requirements is one input to the Router. A requirement is a request for a specified number of channels between two network terminal nodes. A second input is the number and location of network nodes and the link capacity between them. The Router then determines the minimum metric math through the network between those terminal nodes. Path selection can either be constrained by available link channel cross section or be unconstrained. In unconstrained routing, available link and node capacity is not considered when the path is calculated. Conversely, in capacity-constrained routing, only links with available capacity are considered.

SYSTEM CONTROL ANALYSIS AND TRAINING SIMULATION (SCAT)

A HIGHLY INTERACTIVE COMPUTER SIMULATION OF COMMUNICATION NETWORKS

Developed by
James R. Delaney & Torgney Svanes
The MITRE Corporation
Bedford, Massachusetts

Current and proposed military communications networks are required to provide effective service in stressed environments involving unusual traffic demands and losses of network assets. To maintain service under these conditions, a near-real-time flow of network status information sufficient to support quick diagnosis is necessary. Additionally, the human network controller must be experienced in the recognition of network problems and in the selection of appropriate corrective actions. In most cases, the network controller is given little opportunity to gain experience through experimentation, as his only training medium would be the operational network itself.

As part of a continuing effort in the area of system control of communications networks, the MITRE Corporation has supported the development of SCAT, a Systems Control Analysis and Training tool. SCAT is a communications network simulator designed to be an aid in network evaluation and problem diagnosis, the analysis of network response to system control actions, and the training of network controllers. SCAT accomplishes the simulation of a specific network through representation of the network topology and call processing in a series of descriptive tables.

The feature which makes SCAT especially appropriate as a network controller training tool and as a diagnostic support tool is SCAT's comprehensive interactive capability. The controller/trainee or diagnostician interacts with an ongoing network simulation via a repertoire of keyboard-selectable functions from a computer terminal. The interactive capability enables him to

perform on-line experiments through which he can alter the flow of the simulation in response to network developments. Highlights of functions selectable via the terminal keyboard are:

Scenarios: A number of scenario setting functions are incorporated into SCAT's design. These functions include: Satellite outages, Node outages or degradation, Line outages or degradation, Change in traffic patterns. Via the interactive program, these scenarios may be activated at any time during a simulation run. Running the simulation with these scenarios will familiarize the analyst or trainee/controller with network response, and give him experience in diagnosing network problems.

System Control: SCAT's design also incorporates a number of System Control functions, including system control options of present and planned military networks.

Save/Restore Feature: This feature allows the user to save the network status at any given point in time for later restoral. The feature may be used, for example, to compare the relative effectiveness of different control actions against the same scenario.

Network Status and Performance Reports: SCAT features an extensive statistics package which allows the operator to focus his attention on the status and performance of selectable portions of the network.

Key Event Monitoring: This function enables the operator to monitor a multitude of individual call, node-to-node, and network wide conditions. The monitor interrupts the simulation when a preset condition is fulfilled, displays an explanatory message, displays a complete history of the call that has fulfilled the conditions and allows the operator access to the other selectable functions before continuing the simulation.

SCAT is currently operational in an IBM time sharing environment and is programmed in FORTRAN. SCAT can be easily installed on a mini-computer system. In this configuration, SCAT could be deployed for use in the field both for training of network personnel and as a direct operational support. The model has been applied to the European AUTOVON and the NATO Initial Voice Switched Network (IVSN).

DATE
ILMED
-8